St Monica's Catholic Primary School

Hoxton Square, London N1 6NT.

St Monica's E-Safety Policy

Agreed by the Governing Body:
February 2015

Review Date: February 2016

Person(s) Responsible:
Gemma Monaghan (ICT Co-ordinator)

RATIONALE

1 E-SAFETY: THE ISSUES

1.1 Introduction

Nowadays, children are "digital natives", growing up in a world dominated by information and communications technology (ICT) that provides them with access to a wide range of information and increased opportunities for instant communication and social networking.

Using the internet can benefit children's education and give them more opportunities to socialise, but it can also present several risks. Children are often unaware that they are as much at risk online as they are in the real world, and parents and teachers may not be aware of the actions they can take to protect them.

In the face of these risks, parents and schools may deal with the problem by denying or limiting access to the internet; however, this may have little effect as children can access the internet in a range of localities such as libraries, internet cafes and on mobile phones.

It is St Monica's policy that the educational and social benefits of the internet should be promoted, but that this should be balanced against the need to safeguard children. To achieve this, we have developed an e-safety strategy working in partnership with parents.

This document aims to help children and staff use the internet safely and responsibly.

1.2 Information on technologies

Internet technology provides a wide range of activities, including access to information, electronic communications and social networking; each has a clear educational use but also inherent risks for children. The table shown at appendix 4 provides brief details of the various uses of the internet together with their benefits and risks.

1.3 Benefits of ICT

Use of ICT is so universal that it is of huge benefit to children to learn these skills in order to prepare themselves for the working environment; it is important that teachers are aware that the inherent risks are not used to reduce children's use of ICT.

The internet can make a huge contribution to children's education and social development by:

- raising educational attainment, engaging and motivating pupils to learn and improving their confidence

- improving pupil's research and writing skills

- allowing children with disabilities to overcome communications barriers

- enabling children to be taught "remotely", for example children who are unable to attend school

- improving pupil's wellbeing through the social and communications opportunities offered

- providing access to a wide range of educational materials and teaching resources.

1.4 Risks
The risks associated with use of ICT by children can be grouped into 4 categories.

1.4.1 Content
The internet contains a vast store of information from all over the world which is mainly aimed at an adult audience and may be unsuitable for children. There is a danger that children may be exposed to inappropriate images and unsuitable content, or information advocating violence, racism or illegal and anti-social behaviour that they are unable to evaluate in a critical manner.

1.4.2 Contact
Chat rooms and other social networking sites can pose a real risk to children as users can take on an alias rather than their real names and can hide their true identity. The sites may be used by adults who pose as children in order to befriend and gain children's trust (known as "grooming") with a view to harming them.

Children may not be aware of the danger of publishing or disclosing personal information about themselves such as contact details that allow them to be identified or located. They may also inadvertently put other children at risk by posting personal information and photographs without consent.

The internet may also be used as a way of bullying a child, known as cyber bullying. More details on this can be found in section 4.5 of this policy.

1.4.3 Commerce
Children are vulnerable to unregulated commercial activity on the internet that could have serious financial consequences for themselves and their parents. They may give out financial information, for example, their parent's credit card details, in response to offers for goods or services without seeing the fraudulent intent. Disclosing this information can lead to fraud or identity theft.

1.4.4 Culture
Children need to be taught to use the internet in a responsible way, as they may put themselves at risk by:

- becoming involved in inappropriate, anti-social or illegal activities as a result of viewing unsuitable materials or contact with inappropriate people
- using information from the internet in a way that breaches copyright laws
- uploading personal information about themselves, including photographs, on social networking sites without realising they are publishing to a potentially global audience
- cyber bullying (see section 4.5 for further details).

Children may also be adversely affected by obsessive use of the internet that may have a negative impact on their health, social and emotional development and their educational attainment.

2 SCHOOL E-SAFETY STRATEGIES

2.1 Definition and purpose of e-safety

E-safety forms part of the "staying safe" element of the Government's *Every Child Matters* agenda, and all schools have a responsibility under the Children Act 2004 to safeguard and promote the welfare of pupils, as well as owing a duty of care to children and their parents to provide a safe learning environment.

E-safety is a framework of policy, practice, education and technological support that ensures a safe e-learning environment in order to maximise the educational benefits of ICT whilst minimising the associated risks.

Through this e-safety strategy, St Monica's aims to create a safe e-learning environment that:

- promotes the teaching of ICT within the curriculum
- protects children from harm
- safeguards staff in their contact with pupils and their own use of the internet
- ensures the school fulfils its duty of care to pupils
- provides clear expectations for staff and pupils on acceptable use of the internet.

2.2 Elements of e-safety

St Monica's creates an "e-safe" environment for pupils by ensuring that the following aspects are addressed.

2.2.1 Safe systems

St Monica's is linked to the internet via Fronter, the London Grid for Learning platform. Fronter offers a safe e-learning environment by providing filtering software to block access to unsuitable sites, anti-virus software and internet monitoring systems.

2.2.2 Safe practices

Children and staff at St Monica's are made aware of the issues and know what is expected of them in terms of their own acceptable use of the internet and other technologies. Our E-safety policy is consistent with other related school policies such as anti-bullying and behaviour.

2.2.3 Safety awareness

It is vital that children are able to keep themselves and others safe and use the internet responsibly. St Monica's works in partnership with parents, carers and others who have an important role in raising pupils' awareness of the potential dangers of using the internet. In partnership with these other adults, St Monica's helps children to develop their own strategies to avoid these risks and keep safe on-line.

Through annual 'Parent's E-safety workshops' and information sent home in the newsletter, St Monica's ensures that parents and carers are fully aware of e-safety issues so that they can extend e-safety strategies to the home environment.

2.3 Roles and responsibilities

St Monica's e-safety strategy is inclusive of the whole school community and forges links with parents and carers. The strategy has the backing of school governors, is overseen by the head teacher and is fully implemented by all staff, including technical and non-teaching staff.

2.3.1 Head teacher's role

The Head teacher has ultimate responsibility for e-safety issues within St Monica's including:

- the overall development and implementation of the school's e-safety policy
- ensuring that e-safety issues are given a high profile within the school community
- linking with the board of governors and parents and carers to promote e-safety and forward the school's e-safety strategy
- ensuring e-safety is embedded in the curriculum
- deciding on sanctions against staff and pupils who are in breach of acceptable use policies.

2.3.2 Governors' role

The governing body has a statutory responsibility for pupil safety, therefore they are aware of e-safety issues and support the head teacher in the development of the school's e-safety policy and strategy and promote e-safety to parents.

2.3.3 E-safety contact officer's role

The Head teacher and the ICT subject leader are the designated e-safety contact officers.

The e-safety contact officers will:

- develop, implement, monitor and review the school's e-safety policy
- ensure that staff and pupils are aware that any e-safety incident should be reported to them
- provide the first point of contact and advice for school staff, governors, pupils and parents
- liaise with the school's IT manager to ensure they are kept up to date with e-safety issues and to advise of any new trends, incidents and arising problems
- assess the impact and risk of emerging technology and the school's response to this in association with other relevant staff
- raise the profile of e-safety awareness within the school by ensuring access to training and relevant e-safety literature
- ensure that all staff and pupils have read and signed the acceptable use policy (AUP)
- report annually to the board of governors on the implementation of the school's e-safety strategy

- investigate any internet related incidents and co-ordinate any investigation into breaches
- report all incidents and issues meriting further investigation to Camden's e-safety officer.

2.3.4 IT manager's role

At St Monica's, the Hackney Learning Trust IT team are responsible for:

- the maintenance of anti-virus and filtering systems
- carrying out monitoring and audits of networks and reporting breaches to the e-safety contact officer
- supporting any subsequent investigation into breaches and preserving any evidence.

2.3.5 Role of school staff

Teaching staff at St Monica's have a dual role concerning their own internet use and providing guidance, support and supervision for pupils. Their role involves:

- adhering to St Monica's e-safety and acceptable use policy and procedures
- communicating St Monica's e-safety and acceptable use policy to pupils
- keeping pupils safe and ensuring they receive appropriate supervision and support whilst using Fronter in school
- planning use of the internet for lessons and researching on-line materials and resources
- reporting breaches of internet use to the St Monica's e-safety contact officers
- recognising when pupils are at risk from their internet use or have had negative experiences and taking appropriate action, for example referral to the St Monica's e-safety contact officers.

2.3.6 Designated child protection teachers

Where any e-safety incident has serious implications for the child's safety or well-being, the matter should be referred to the St Monica's e-safety contact officers who will decide whether or not a referral should be made to Safeguarding and Social Care or the Police.

2.4 Pupils with special needs

Pupils with learning difficulties or disability may be more vulnerable to risk from use of the internet and will require additional guidance on e-safety practice as well as closer supervision.
The Inclusion Manager is responsible for providing extra support for these pupils and should:

- link with the St Monica's e-safety contact officers to discuss and agree whether the mainstream safeguarding systems on Fronter are adequate for pupils with special needs
- where necessary, liaise with the e-safety contact officers and the Schools IT team to discuss any requirements for further safeguards to Fronter or tailored resources and materials in order to meet the needs of pupils with special needs

- ensure that the St Monica's e-safety policy is adapted to suit the needs of pupils with special needs

- liaise with parents, carers and other relevant agencies in developing e-safety practices for pupils with special needs

- keep up to date with any developments regarding emerging technologies and e-safety and how these may impact on pupils with special needs.

2.5 Working with parents and carers

At St Monica's we are aware that most children will have internet access at home and might not be as closely supervised in its use as they would be at school.

Therefore, parents and carers need to know about the risks so that they are able to continue e-safety education at home and regulate and supervise children's use as appropriate to their age and understanding.

St Monica's holds an annual Parent's e-safety workshops to discuss e-safety issues and any concerns parents or carers may have regarding their child's safety on the internet. In addition, e-safety advice is annually sent out to all parents/carers through the newsletter and supplemented by regular updates. This ensures parents are aware of e-safety issues and support them in reinforcing e-safety messages at home.

Parents are provided with information on Computing learning and the school's e-safety policy when they are asked to sign acceptable use agreements on behalf of their child. This means that parents are fully aware of their child's level of internet use within the school as well as the school's expectations regarding their behaviour.

3 E-SAFETY POLICIES

3.1 Accessing and monitoring the system

- Access to the internet server and Virtual Learning Environment (VLE) at St Monica's is via individual log-ins and passwords. Each child and member of staff is issued with their own usernames and passwords.

- The e-safety contact officers have a record of all log-ins used within the school for the purposes of monitoring and auditing internet activity.

- The e-safety contact officers and teaching staff carefully consider the location of computer terminals in classrooms and teaching areas in order to allow an appropriate level of supervision of pupils.

3.2 Acceptable use policies

- At St Monica's, acceptable use agreements are signed by parents on their child's behalf at the same time that they give consent for their child to have access to the Virtual Learning Environment in school (see appendix 1).
- Staff are expected to sign an acceptable use policy on appointment and this will be integrated into their general terms of employment (see appendix 2).

A copy of each signed acceptable use agreement is kept in the school office.

3.3 Teaching e-safety

3.3.1 Responsibility

One of the key features of St Monica's e-safety strategy is teaching pupils to protect themselves and behave responsibly while on-line. There is an expectation that over time, pupils will take increasing responsibility for their own behaviour and internet use so that they can be given more freedom to explore systems and applications with a lessening amount of supervision from staff.

Overall responsibility for the design and co-ordination of e-safety education lies with the e-safety contact officers, but all teaching staff should play a role in delivering e-safety messages. The e-safety contact officers are responsible for ensuring that all staff have the knowledge and resources to enable them to do so.

3.3.2 Content

Pupils are taught:

- the benefits and risks of using the internet
- how their behaviour can put themselves and others at risk
- what strategies they can use to keep themselves safe
- what to do if they are concerned about something they have seen or received via the internet
- who to contact to report concerns
- that the school has a "no blame" policy so that pupils are encouraged to report any e-safety incidents
- that the school has a "no tolerance" policy regarding cyber bullying
- that behaviour that breaches acceptable use policies will be subject to sanctions and disciplinary action
- the internet and Virtual Learning Environment should only be used for educational purposes
- the internet server has been designed so that use is monitored and that access to some sites are blocked

• the school's policy on mobile phones whilst in school.

3.3.3 Delivering e-safety messages

• Teachers are primarily responsible for delivering an ongoing e-safety education in the classroom as part of the curriculum. At St Monica's children are reminded to be S.M.A.R.T (see appendix 5)

• An annual E-Safety week is held at St Monica's, allowing time for both whole-school and individual class e-safety education

• Rules regarding safe internet use are posted up in all classrooms and teaching areas where computers are used to deliver lessons

• The start of every lesson where computers are being used should be an opportunity to remind pupils of expectations on internet use and the need to follow basic principles in order to keep safe

• Teachers may wish to use PSHE lessons as a forum for discussion on e-safety issues to ensure that pupils understand the risks and why it is important to regulate their behaviour whilst on-line

• Teachers should ensure that the school's policy on pupils' use of their own mobile phones in school is adhered to.

3.4 ICT and safe teaching practice

School staff need to be aware of the importance of maintaining professional standards of behaviour with regards to their own internet use, particularly in relation to their communications with pupils.

The following points should be followed by staff to ensure that their behaviour is not open to misinterpretation and to safeguard them from misplaced or malicious allegations.

• Photographic and video images of pupils should only be taken by staff in connection with educational purposes, for example school trips

• Staff should always use school equipment and only store images on the school computer system, with all other copies of the images erased

• Staff should take care regarding the content of and access to their own social networking sites and take all reasonable steps to ensure that pupils and parents cannot gain access to these

• Staff should ensure that any materials published on their own social networking sites are neither inappropriate nor illegal.

• Staff should be particularly careful regarding any comments to do with the school or specific pupils that are communicated over the internet; remarks that are private may go to a wider audience and raise questions regarding confidentiality

• Staff should not engage in any conversation with pupils via instant messaging or social networking sites as these may be misinterpreted or taken out of context

• Where staff need to communicate with pupils regarding school work, this should be via the VLE and messages should be carefully written to ensure that they are clear, unambiguous and not open to any negative interpretation

• When making contact with parents or pupils by telephone, staff should only use school equipment. Pupil or parent numbers should not be stored on a staff member's personal mobile phone and staff should avoid lending their mobile phones to pupils

• Staff should ensure that personal data relating to pupils is stored securely and encrypted if taken off the school premises

• Where staff are using mobile equipment such as laptops provided by the school, they should ensure that the equipment is kept safe and secure at all times.

3.5 Safe use of ICT

3.5.1 Internet and search engines

• When using the internet, children should receive the appropriate level of supervision for their age and understanding. Teachers should be aware that often, the most computer-literate children are the ones who are most at risk

• At St Monica's, children should be supervised at all times when using the internet

• Pupils should not be allowed to aimlessly "surf" the internet and all use should have a clearly defined educational purpose.

• Children are not allowed to use search engines not specifically designed for children such as www.google.co.uk. Children are only allowed to use the following search engines:

www.ajkids.com

www.kidsclick.org

www.yahooligans.com

www.thinkquest.org

• Despite filtering systems, it is still possible for pupils to inadvertently access unsuitable websites; to reduce risk, teachers should plan use of internet resources ahead of lessons by checking sites and storing information off-line where possible

• Where teachers require access to blocked websites for educational purposes, this should be discussed and agreed with the e-safety contact officers, who will liaise with the Schools IT team for temporary access.

3.5.2 Evaluating and using internet content

As the information generated by internet searches could be vast, and much of it irrelevant to the subject being taught, teachers should teach pupils good research skills that help them to maximise the resource. They should also be taught how to critically evaluate the information retrieved by:

- questioning the validity of the source of the information; whether the author's view is objective and what authority they carry
- carrying out comparisons with alternative sources of information
- considering whether the information is current and whether the facts stated are correct.

3.5.3 Emails

The VLE hosts an email system that allows pupils to send emails to others within the school or to approved email addresses externally.

- Access to and use of personal email accounts on the VLE is forbidden and may be blocked. This is to protect pupils from receiving unsolicited mail and preserve the safety of the system from hacking and viruses
- Emails should only be sent via VLE to addresses within the school system or an approved external address
- Where teachers wish to add an external email address, this must be for a clear educational purpose and must be discussed with the e-safety contact officers who will liaise with the Schools IT team
- Pupils are taught not to disclose personal contact details for themselves or others such as addresses or telephone numbers via email correspondence
- All email communications should be polite; if a pupil receives an offensive or distressing email, they should be instructed not to reply and to notify the responsible teacher immediately
- Pupils should be warned that any bullying or harassment via email will not be tolerated and will be dealt with in accordance with the school's anti-bullying policy
- Users should be aware that use of e-mail via the VLE is for the purposes of education or school business only, and all emails may be monitored
- Access to email systems by pupils should be via a class email address only
- All email messages sent by pupils in connection with school business must be checked and cleared by the responsible teacher
- Apart from the head teacher, individual email addresses for staff or pupils should not be published on the school website
- Pupils are taught to be wary of opening attachments to emails where they are unsure of the content or have no knowledge of the sender.

3.5.4 Social networking sites, newsgroups and forums

Social networking sites such as Facebook, MySpace and Bebo allow users to publish information about them to be seen by anyone who has access to the site. These sites have been blocked at St Monica's but some pupils may use these sites at home.

• Access to unregulated public social networking sites, newsgroups or forums are blocked

• Where a clear educational use for these sites for on-line publishing is identified, they should only use approved sites such as those provided by the London Grid for Learning

• Any use of these sites should be strictly supervised by the responsible teacher

• Pupils are warned that any bullying or harassment via social networking sites will not be tolerated and will be dealt with in accordance with the school's anti-bullying policy

• In order to teach pupils to stay safe on social networking sites outside of school, they are advised:

o not to give out personal details to anyone on-line that may help to identify or locate them or anyone else, for example home address, name of school or clubs attended

o not to upload personal photos of themselves or others onto sites and to take care regarding what information is posted

o to behave responsibly whilst on-line and keep communications polite

o not to respond to any hurtful or distressing messages but to let their parents or carers know so that appropriate action can be taken.

3.5.5 Chat rooms and instant messaging

Chat rooms are internet sites where users can join in "conversations" on-line; instant messaging allows instant communications between two people on-line. In most cases, pupils will use these at home although Fronter does host these applications.

• Access to public or unregulated chat rooms will be blocked except for the site hosted by Fronter, which is to be used for educational purposes only

• Pupils are warned that any bullying or harassment via chat rooms or instant messaging taking place within or out of school will not be tolerated and will be dealt with in accordance with the school's anti-bullying policy

• In order to teach pupils to stay safe whilst using chat rooms outside of school, they are advised:

- not to give out personal details to anyone on-line that may help to identify or locate them or anyone else
- only use moderated chat rooms that require registration and are specifically for their age group
- not to arrange to meet anyone whom they have only met on-line
- to behave responsibly whilst on-line and keep communications polite

- not to respond to any hurtful or distressing messages but to let their parents or carers know so that appropriate action can be taken.

3.5.6 Video conferencing

Video conferencing enables users to communicate face-to-face via the internet using web cameras.

• Video conferencing is not carried out by pupils at St Monica's.

• Teachers should avoid using other webcam sites on the internet due to the risk of them containing links to adult material. In the event that teachers do use other webcam sites, this should be discussed and agreed in advance with the Schools IT team

• Pupil use of video conferencing should be for educational purposes and should be supervised as appropriate to their age. Pupils must ask permission from the responsible teacher before making or receiving a video conference call

• Teachers should ensure that pupils are appropriately dressed during any photography or filming and equipment must not be used in changing rooms or toilets

• Photographic or video devices may be used by teachers only in connection with educational activities including school trips

• Photographs and videos may only be downloaded onto the school's computer system with the permission of the e-safety contact officers and should never enable individual pupils' names or other identifying information to be disclosed.

3.5.7 School website

• Content should not be uploaded onto the school website unless it has been authorised by the e-safety contact officers, who are responsible for ensuring that content is accurate, suitable for the purpose and audience, and does not breach copyright or intellectual property law

• St Monica's has designated named persons to have responsibility for uploading materials onto the website

• To ensure the privacy and security of staff and pupils, the contact details on the website should be the school address, email and telephone number. No contact details for staff or pupils should be contained on the website

• Children's full names should never be published on the website

• Links to any external websites should be regularly reviewed to ensure that their content is appropriate for the school and the intended audience.

3.5.8 Photographic and video images

• Where the school uses photographs and videos of pupils for publicity purposes, for example on the school website, images should be carefully selected so that individual pupils cannot be easily identified. It is recommended that group photographs are used

• Where photographs or videos of children are used, written permission must be obtained first from their parents or carers, who should be informed of the purpose of the image and where it will appear

• Children's full names should never be published where their photograph or video is being used

• Staff should ensure that children are suitably dressed to reduce the risk of inappropriate use of images

• Images should be securely stored only on the school's computer system and all other copies deleted.

• Stored images should not be labelled with the child's full name.

3.5.9 Pupil's own mobile phone/handheld systems

Pupils are only permitted to have a mobile phone at school with them if permission has been granted by their parents and acknowledged by the class teacher. Pupils must hand their mobile phones to their teacher at the start of the school day to be stored in a secure and safe place within the classroom. The mobile phones are returned to pupils at the end of the day (see appendix 6)

4 RESPONDING TO INCIDENTS

4.1 Policy statement

• All incidents and complaints relating to e-safety and unacceptable internet use will be reported to the e-safety contact officers in the first instance. All incidents, whether involving pupils or staff, must be recorded by the e-safety contact officers on the e-safety incident report form (appendix 3).

• A copy of the incident record should be emailed to **Camden's designated e-safety officer at jenni.spencer@camden.gov.uk.**

• Where the incident or complaint relates to a member of staff, the matter must always be referred to the head teacher for action. Incidents involving the Head teacher should be reported to the chair of the board of governors.

• The school's e-safety contact officers should keep a log of all e-safety incidents and complaints and regularly review the information for evidence of emerging patterns of individual behaviour or weaknesses in the school's e-safety system, and use these to update the e-safety policy.

• E-safety incidents involving safeguarding issues, for example contact with inappropriate adults, should be reported to the Designated Child Protection officer, who will make a decision as to whether or not to refer the matter to the police and/or Safeguarding and Social Care in conjunction with the Head teacher.

Although it is intended that e-safety strategies and policies should reduce the risk to pupils whilst on-line, this cannot completely rule out the possibility that pupils may access unsuitable material on the internet. Neither the school nor the London Borough of Camden can accept liability for

material accessed or any consequences of internet access, but all reasonable precautions will be taken to ensure a safe e-learning environment.

4.2 Unintentional access of inappropriate websites

• If a pupil or teacher accidently opens a website that has content which is distressing or upsetting or inappropriate to the pupils' age, teachers should immediately (and calmly) close or minimise the screen.

• Teachers should reassure pupils that they have done nothing wrong and discuss the incident with the class to reinforce the e-safety message and to demonstrate the school's "no blame" approach.

• The incident should be reported to the e-safety contact officers and details of the website address and URL provided.

• The e-safety contact officers should liaise with the Schools IT team to ensure that access to the site is blocked and the school's filtering system reviewed to ensure it remains appropriate.

4.3 Intentional access of inappropriate websites by a pupil

• If a pupil deliberately accesses inappropriate or banned websites, they will be in breach of the acceptable use policy and subject to appropriate sanctions (see section 5).

• The incident should be reported to the e-safety contact officers and details of the website address and URL recorded.

• The e-safety contact officers should liaise with the Schools IT team to ensure that access to the site is blocked.

• The pupil's parents should be notified of the incident and what action will be taken.

4.4 Inappropriate use of ICT by staff

• If a member of staff witnesses misuse of ICT by a colleague, they should report this to the head teacher and the e-safety contact officers immediately.

• The e-safety contact officers should notify the Schools IT team so that the computer or laptop is taken out of use and securely stored in order to preserve any evidence. A note of any action taken should be recorded on the e-safety incident report form.

• The e-safety contact officers should arrange with the Schools IT team to carry out an audit of use to establish which user is responsible and the details of materials accessed.

• Once the facts are established, the head teacher should take any necessary disciplinary action against the staff member and report the matter to the school governors and the police where appropriate.

• If the materials viewed are illegal in nature the head teacher should report the incident to the police and follow their advice, which should also be recorded on the e-safety incident report form.

4.5 Cyber bullying

4.5.1 Definition and description

Traditionally, bullying took place face to face in the physical world; on-line, bullying can take on a new dimension with technologies such as email, mobile phones and social networking sites used as a platform to hurt, humiliate, harass or threaten victims.

Cyber bullying is defined as the use of ICT to deliberately hurt or upset someone. Unlike physical forms of bullying, the internet allows bullying to continue past school hours and invades the victim's home life and personal space. It also allows distribution of hurtful comments and material to a wide audience.

Cyber bullying is extremely prevalent as pupils who would not consider bullying in the physical sense may find it easier to bully through the internet, especially if it is thought the bullying may remain anonymous.

Bullying may take the form of:

- rude, abusive or threatening messages via email or text
- posting insulting, derogatory or defamatory statements on blogs or social networking sites
- setting up websites that specifically target the victim
- making or sharing derogatory or embarrassing videos of someone via mobile phone or email (for example, "happy slapping").

Cyber bullying can affect pupils and staff members. Often, the internet medium used to perpetrate the bullying allows the bully to remain anonymous. In extreme cases, cyber bullying could be a criminal offence under the Harassment Act 1997 or the Telecommunications Act 1984.

4.5.2 Dealing with incidents

The following covers all incidents of bullying that involve pupils at St Monica's, whether or not they take place on school premises or outside school.

- School anti-bullying and behaviour policies and acceptable use policies cover the issue of cyber bullying and set out clear expectations of behaviour and sanctions for any breach.

• Any incidents of cyber bullying should be reported to the e-safety contact officers who will record the incident on the incident report form and ensure that the incident is dealt with in line with the school's anti-bullying policy.

Incidents will be monitored and the information used to inform the development of anti-bullying policies.

• Where incidents are extreme, for example threats against someone's life, or continue over a period of time, consideration should be given to reporting the matter to the police as in these cases, the bullying may be a criminal offence.

• As part of e-safety awareness and education, pupils are told of the "no tolerance" policy for cyber bullying and encouraged to report any incidents to their teacher.

• Pupils should be taught:

- to only give out mobile phone numbers and email addresses to people they trust
- to only allow close friends whom they trust to have access to their social networking page
- not to respond to offensive messages
- to report the matter to their parents and teacher immediately.

• Evidence of bullying, for example texts, emails or comments on websites should be preserved by the young person as evidence.

4.5.3 Action by service providers

All website providers and mobile phone companies are aware of the issue of cyber bullying and have their own systems in place to deal with problems, such as tracing and blocking communications. Teachers or parents can contact providers at any time for advice on what action can be taken.

• Where the bullying takes place by mobile phone texts, the mobile phone company can be contacted to ask them to trace the calls and ensure that any further calls and texts from that number are blocked. The pupil should also consider changing their phone number.

• Where the bullying takes place by email, and the messages are being sent from a personal email account, contact the service provider so that the sender can be traced and further emails from the sender blocked. The pupil should also consider changing email address.

• Where bullying takes place in chat rooms, the pupil should leave the chat room immediately and seek advice from parents or teachers. Bullying should be reported to any chat room moderator to take action.

• Where bullying involves messages on social networking sites or blogs, contact the website provider to request that the comments are removed. In extreme cases, the bully's access to the site can be blocked.

• Parents should be notified of any incidents and advised on what measures they can take to block any offensive messages on computers at home.

4.5.4 Cyber bullying of teachers

• The e-safety contact officers are aware that teachers may become victims of cyber bullying by pupils. Because of the duty of care owed to staff, the Head teacher will ensure that teachers are able to report incidents in confidence and receive adequate support, including taking any appropriate action against pupils.

• The issue of cyber bullying of teachers should be incorporated into any anti-bullying policies, education programme or discussion with pupils so that they aware of their own responsibilities.

• Incidents of cyber bullying involving teachers should be recorded and monitored by the e-safety contact officers in the same manner as incidents involving pupils.

• Teachers should follow the guidance on safe ICT use in section 3.4 of this policy and avoid using their own mobile phones or personal email addresses to contact parents or pupils so that no record of these details becomes available.

• Personal contact details for teachers should not be posted on the school website or in any other school publication.

• Teachers should follow the advice above on cyber bullying of pupils and not reply to messages but report the incident to the e-safety contact officers immediately.

4.6 Risk from inappropriate contacts

Teachers may be concerned about a pupil being at risk as a consequence of their contact with an adult they have met over the internet. The pupil may report inappropriate contacts or teachers may suspect that the pupil is being groomed or has arranged to meet with someone they have met on-line.

• All concerns around inappropriate contacts should be reported to Designated Child Protection officer.

• The Designated Child Protection officer should discuss the matter with the referring teacher and where appropriate, speak to the pupil involved, before deciding whether or not to make a referral to Safeguarding and Social Care and/or the police.

• The police should always be contacted if there is a concern that the child is at immediate risk, for example if they are arranging to meet the adult after school.

• The Designated Child Protection officer can seek advice on possible courses of action from Camden's e-safety officer in Safeguarding and Social Care.

• Teachers should advise the pupil how to terminate the contact and change contact details where necessary to ensure no further contact.

• The Designated Child Protection officer and the e-safety contact officers should always notify the pupil's parents of any concerns or incidents and where appropriate, arrange to meet with them discuss what action they can take to ensure their child's safety.

• Where inappropriate contacts have taken place using school ICT equipment or networks, the e-safety contact officers should make a note of all actions taken and contact the Schools IT team to ensure that all evidence is preserved and that an audit of systems is carried out to ensure that the risk to other pupils is minimised.

4.7 Risk from contact with violent extremists

Many extremist groups who advocate violence use the internet as a means of either inciting violence against specific groups or providing information on preparing explosives or carrying out terrorist acts. Because of their personal circumstances, some young people may be susceptible to these influences.

• Staff need to be aware of those pupils who are being targeted by or exposed to harmful influences from violent extremists via the internet. Pupils and staff should be warned of the risks of becoming involved in such groups and informed that accessing such websites is against school policies.

• The school should ensure that adequate filtering is in place and review filtering in response to any incident where a pupil or staff member accesses websites advocating violent extremism.

• All incidents should be dealt with as a breach of the acceptable use policies and the school's behaviour and staff disciplinary procedures should be used as appropriate.

• The e-safety contact officers and the Designated Child Protection officer should record and review all incidents in order to establish whether there are any patterns of extremist groups targeting the school and whether current school procedures are robust enough to deal with the issue.

5 SANCTIONS FOR MISUSE OF SCHOOL ICT

5.1 Sanctions for pupils

5.1.1 Category A infringements

These are basically low-level breaches of acceptable use agreements such as:

• use of non-educational sites during lessons

• unauthorised use of email or mobile phones

• unauthorised use of prohibited sites for instant messaging or social networking.

The class teacher is to be notified and they should in turn notify the e- safety contact officers. Pupils, and if the teacher deems it necessary, the child's parent/carer should be reminded of the acceptable use agreement.

5.1.2 Category B infringements

These are persistent breaches of acceptable use agreements following warnings and use of banned sites or serious breaches of e-safety policy that are non-deliberate, such as:

• continued use of non-educational sites during lessons

- continued unauthorised use of email or mobile phones
- continued use of prohibited sites for instant messaging or social networking
- use of file sharing software
- accidentally corrupting or destroying other people's data without notifying staff
- accidentally accessing offensive material without notifying staff.

The class teacher is to be notified and they should in turn notify the e- safety contact officers. Parents should be contacted and the pupil should have loss of computer/internet access for a period of time.

5.1.3 Category C infringements

These are deliberate actions that either negatively affect Fronter or are serious breaches of acceptable use agreements or anti-bullying policies, such as:

- deliberately bypassing security or access
- deliberately corrupting or destroying other people's data or violating other's privacy
- cyber bullying
- deliberately accessing, sending or distributing offensive material
- purchasing or ordering items over the internet
- transmission of commercial or advertising material.

The pupil(s) should be referred to the Head teacher and the other e-safety contact officer should be notified. Parents are to be contacted to discuss the infringements and the appropriate sanctions.

5.1.4 Category D infringements

These are continued serious breaches of acceptable use agreements following warnings or deliberately accessing and distributing banned or illegal material which may result in a criminal offence, such as:

- persistent and/or extreme cyber bullying
- deliberately accessing, downloading or disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- receipt or transmission of material that infringes the copyright of other people or is in breach of the Data Protection Act
- bringing the school name into disrepute.

The pupil(s) should be referred immediately to the Head teacher. Parents are to be contacted to discuss the infringements and the appropriate sanctions.

5.2 Sanctions for staff

These should reflect the seriousness with which any breach of acceptable use policies by staff members will be viewed given their position of trust and the need to ensure acceptable standards of behaviour by adults who work with children.

5.2.1 Category A infringements

These are minor breaches of the school's acceptable use policy which amount to misconduct and will be dealt with internally by the Head teacher.

- excessive use of internet for personal activities not connected to professional development
- use of personal data storage media (eg: removable memory sticks) without carrying out virus checks
- any behaviour on the world wide web that compromises the staff member's professional standing in the school and community, for example inappropriate comments about the school, staff or pupils or inappropriate material published on social networking sites
- sharing or disclosing passwords to others or using other user's passwords
- breaching copyright or licence by installing unlicensed software.

5.2.2 Category B infringements

These infringements involve deliberate actions that undermine safety on Fronter and activities that call into question the person's suitability to work with children. They could represent gross misconduct requiring a strong response and possible referral to other agencies such as the police or Safeguarding and Social Care. Such matters would be referred to the Head teacher who would decide on the appropriate course of action in line with school policies.

- serious misuse of or deliberate damage to any school computer hardware or software, for example deleting files, downloading unsuitable applications
- any deliberate attempt to breach data protection or computer security rules, for example hacking
- deliberately accessing, downloading or disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- receipt or transmission of material that infringes the copyright of other people or is in breach of the Data Protection Act.

Appendix 1

Acceptable use policy for St Monica's Primary School pupils

Name:

School:

Class:

I want to stay safe while I am using a computer and I know that anything I do on the computer may be seen by someone else.

I will:

- keep my password a secret
- only open pages which my teacher has said are okay
- tell my teacher if anything makes me feel scared or uncomfortable
- make sure all the messages I send are polite
- tell my teacher if I get a message which makes me feel scared or uncomfortable
- not reply to any message which makes me feel upset or uncomfortable
- not give my mobile number, home number or address to anyone who is not a real friend
- only email people I know or if my teacher agrees
- only use my school email address
- talk to my teacher before using anything on the internet
- not tell people about myself on-line (I will not tell them my name, anything about where I live or where I go to school)
- not load photographs of myself onto the computer

• never agree to meet a stranger.

Parents

□ I have read the above school rules for responsible internet use and agree that my child may have access to the Virtual Learning Environment. I understand that the school will take all reasonable precautions to ensure pupils do not have access to inappropriate websites, and that the school cannot be held responsible if pupils do access inappropriate websites.
□ I agree that my child's work can be published on the school website.
□ I agree that photographs that include my child may be published but that any photography will not be accompanied by my child's full name.

Signed:

Date:

Appendix 2

Acceptable use policy for St Monica's Primary School staff

Access and professional use

• All computer networks and systems belong to the school and are made available to staff for educational, professional and administrative purposes only.

• Staff are expected to abide by all school e-safety rules and the terms of this acceptable use policy. Failure to do so may result in disciplinary action being taken.

• The school reserves the right to monitor internet activity and examine and delete files from the school's system.

• Staff have a responsibility to safeguard pupils in their use of the internet and reporting all e-safety concerns to the e-safety contact officers.

• Copyright and intellectual property rights in relation to materials used from the internet must be respected.

• E-mails and other written communications must be carefully written and polite in tone and nature.

• Anonymous messages and the forwarding of chain letters are not permitted.

• Staff should only access internet sites in school that are accessible using the school's filtering system. The use of chat rooms and access to personal email accounts or social networking sites and blogs using school equipment is not allowed.

Data protection and system security

• Staff should ensure that any personal data sent over the internet will be encrypted or sent via secure systems. Where personal data is taken off the school premises via laptops and other mobile systems, the information must be encrypted beforehand.

• Use of any portable media, not supplied by school, such as USB sticks or CD-ROMS is not allowed unless permission has been given by the Schools IT team and a virus check has been carried out.

• Downloading executable files or unapproved system utilities will not be allowed and all files held on Fronter will be regularly checked.

• Sharing and use of other people's log-ins and passwords is forbidden. Users should ensure that they log-out when they have finished using a computer terminal.

• Files should be saved, stored and deleted in line with the school policy.

Personal use

• Staff should not browse, download or send material that could be considered offensive to colleagues and pupils or is illegal.

• Staff should not allow school equipment or systems to be used or accessed by unauthorised persons and keep any school computers or hardware used at home safe.

• Staff should ensure that personal websites or blogs do not contain material that compromises their professional standing or brings the school's name into disrepute.

• Fronter may not be used for private purposes without permission from the Head teacher.

I have read the above policy and agree to abide by its terms.

Name:

Signed:

Date:

Appendix 3

E-safety incident report form

This form should be kept on file and a copy emailed to Camden's e-safety officer at **jenni.spencer@camden.gov.uk**

School's details:

Name of school/organisation: St Monica's

Address:

Name of e-safety contact officers:

Contact details:

Details of incident:

Date happened:

Time:

Name of person reporting incident:

If not reported, how was the incident identified?

Where did the incident occur? (Please tick)

□ In school/service setting □ Outside school/service setting

Who was involved in the incident?

□ child/young person □ staff member □ other (please specify

Type of incident:

□ bullying or harassment (cyber bullying)

□ deliberately bypassing security or access

□ hacking or virus propagation

□ racist, homophobic, religious hate material

□ terrorist material

□ child abuse images

□ on-line gambling

□ other (please specify)

Description of incident

Nature of incident:

□ ***Deliberate access***

Did the incident involve material being;

□ created □ viewed □ printed □ shown to others

□ transmitted to others □ distributed

Could the incident be considered as;

□ harassment □ grooming □ cyber bullying □ breach of AUP

OR

□ ***Accidental access***

Did the incident involve material being;

□ created □ viewed □ printed □ shown to others

□ transmitted to others □ distributed

Action taken:

□ Staff

□ incident reported to head teacher

□ advice sought from Safeguarding and Social Care

□ referral made to Safeguarding and Social Care

□ incident reported to police

□ incident reported to Schools IT team

□ disciplinary action to be taken

□ e-safety policy to be reviewed/amended

Please detail any specific action taken (ie: removal of equipment):

□ Child/young person

□ incident reported to head teacher

□ advice sought from Safeguarding and Social Care

□ referral made to Safeguarding and Social Care

□ incident reported to police

□ incident reported to social networking site

□ incident reported to Schools IT team

□ child's parents informed

□ disciplinary action to be taken

□ child/young person debriefed

□ e-safety policy to be reviewed/amended

Outcome of incident/investigation:

Appendix 4

Description of ICT Applications

Technology/ Application	Description/ Usage	Benefits	Risks
Internet	• Enables the storage, publication and retrieval of a vast range of information • Supports communication systems	• Provides access to a wide range of educational materials, information and resources to support learning • Enables pupils and staff to communicate widely with others • Enhances school's management information and business administration systems.	• Information is predominantly for an adult audience and may be unsuitable for children • The vast array of information makes retrieval difficult without good research skills and ability to critically evaluate information • Access to sites promoting illegal or anti-social activities, extreme views or commercial and gambling sites.
Email	• Allows written communication over the network and the ability to attach documents.	• Enables exchange of information and ideas and supports collaborative working. • Enhances written communication	• Difficulties controlling contacts and content • Use as a platform for bullying and harassment • Risks from unwanted spam

peer networking)	computer capability, networks and file storage. • Used to share music, video and other materials.	within a community of peers with similar interests and exchange materials.	copyright infringement. • Exposure to unsuitable or illegal materials. • Computers are vulnerable to viruses and hacking.
Mobile phones and multi-media equipment	• Mobile phones now carry other functions such as cameras, video-messaging and access to internet and email.	• Provide children with a good means of communication and entertainment. • They can also keep children safe and allow them to be contacted or stay in contact.	• Their mobile nature makes supervision of use difficult leading to risks of unsuitable contacts or exposure to unsuitable material on the internet or through messaging. • Risk from

Appendix 5

S.M.A.R.T

Safe: Keep safe by being careful not to give out personal information when you're chatting or posting online. Personal information includes your email address, phone number and password.

Meeting: Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then only when they can be present. Remember online friends are still strangers even if you have been talking to them for a long time.

Accepting: Accepting emails, IM messages, or opening files, pictures or texts from people you don't know or trust can lead to problems – they may contain viruses or nasty messages!

Reliable: Someone online might lie about who they are and information on the internet may not be true. Always check information with other websites, books or someone who knows. If you like chatting online it's best to only chat to your real world friends and family

Tell: Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online (Make link to text messaging)

Appendix 6

Mobile Phone Agreement

Home/School agreement for bringing a mobile phone to school

3.5.9 Pupil's own mobile phone/handheld systems

Pupils are only permitted to have a mobile phone at school with them if permission has been granted by their parents and acknowledged by the class teacher. Pupils must hand their mobile phones to their teacher at the start of the school day to be stored in a secure and safe place within the classroom. The mobile phones are returned to pupils at the end of the day

As a general rule, pupils are not allowed to have mobile telephones in school. We recognise that, from time to time, circumstances may arise where a parent expressly wishes for their child to bring a mobile phone to school. In these cases we are happy to grant permission, subject to the following restrictions:-

 Prior permission is sought by the parent and a Home/School agreement signed

 The telephone is handed in to the child's class teacher, with a note of the child's name, at the beginning of school. It will be held safely until it can be collected when the child leaves school.

 The school does not accept responsibility for the security of mobile telephones even when they are handed in to the teacher. Neither will valuable curriculum time be spent in tracking down missing phones.

 Mobile phones must be switched off whilst on school premises unless being used with permission from a member of staff

 Under no circumstances may images be taken on mobile phones.

 If a mobile phone is being used inappropriately it will be taken away from the pupil and kept until an adult collects it.

I have read the conditions above and I understand that if my child brings a mobile phone to school that the school accepts no responsibility for it.

Name of child _____

Signed _____ **(child) Date** _____

Signed _____ **(parent) Date** _____

Signed _____ **(school) Date** _____