St Mary's Church of England Primary School
Online Safety Policy
September 2016

Contents

Appendices:

1 Introduction

1.1 Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Mary's CE Primary School with respect to the use of IT-based technologies.
- Safeguard and protect the children and staff of St Mary's CE Primary School.
- Assist school staff working with children to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use.
- Have clear structures to deal with online abuse such as online bullying which are cross referenced with other school policies.
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with students.

1.2 Benefits of using the internet and 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 pupils' 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.

1.3 Risks of using the internet and ICT

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 our 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, our school is developing an online strategy working in partnership with parents.

Appendix 5 provides brief details of the various uses of the internet together with their benefits and risks.

The main areas of risk for our school community can be summarised as follows:

Content

- Exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), information advocating violence, racism or illegal and anti-social behaviour and substance abuse;
- Lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- Hate sites;
- Content validation: how to check authenticity and accuracy of online content.

Contact

- Other users taking on an alias rather than their real names, therefore hiding their true identity;
- Grooming, adults who pose as children in order to befriend and gain children's trust with a view to sexually abusing them;
- Online bullying (cyber bullying) in all forms;
- Identity theft (including 'frape' (hacking Facebook profiles)) and sharing passwords.

Conduct

- Becoming involved in inappropriate, anti-social or illegal activities.
- Privacy issues, including disclosure of personal information. Uploading personal information about themselves, including photographs;
- Digital footprint and online reputation;
- Health and well-being (amount of time spent online (Internet or gaming));
- Sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images);
- Extremism;
- Copyright (little care or consideration for intellectual property and ownership – such as music and film).

Commerce

- Giving out financial information for example their parents' credit card details;
- Disclosing information that can lead to fraud or identity theft;

(Ref Ofsted 2013)

1.4 Scope

This policy applies to all members of St Mary's CE Primary School (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of St Mary's CE Primary School Computing systems, both in and out of school.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of Online bullying, or other online safety incidents covered by this policy, which may take place outside of school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate online safety behaviour that take place out of school.

1.5 Roles and Responsibilities

A successful online strategy needs to be inclusive of the whole school community and forge links with parents and carers. Our strategy has the backing of school governors, is overseen by the Head of School and is fully implemented by all staff, including technical and non-teaching staff through policies, parent meetings and staff meetings.

Role	Key Responsibilities
Head of School	• To take overall responsibility for online safety provision; • To take overall responsibility for data and data security; • To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements (school uses London Grid for Learning); • To be responsible for ensuring that staff receive suitable training to carry out their online safety roles and to train other colleagues, as relevant; • To ensure that online safety is given a high profile within the school community. • To be aware of procedures to be followed in the event of a serious online safety incident; • To link with the Board of Governors and parents and carers to promote online safety and forward the school's online safety policy; • To ensure online safety is embedded in the curriculum; • To decide on sanctions against staff and pupils who are in breach of acceptable use policies. • Liaises with school Computing technical staff

Role	Key Responsibilities

Designated child protection officer	• To ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident;
	• Is regularly updated in online safety issues and legislation, and be aware of the potential for serious child protection issues to arise from:
	  • sharing of personal data
	  • access to illegal / inappropriate materials
	  • inappropriate on-line contact with adults / strangers
	  • potential or actual incidents of grooming
	  • Online bullying and use of social media.

Online Safety Co-ordinator	• To develop, monitor and review the school's online safety policy;
	• To oversee the delivery of the online safety element of the computing curriculum;
	• To make sure staff and pupils are aware that any online safety incident should be reported to them;
	• To take day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents;
	• To promotes an awareness and commitment to online safeguarding throughout the school community;
	• To make sure that online safety education is embedded across the curriculum;
	• To communicate regularly with SLT and the Governors to discuss current issues;
	• To ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident;
	• To facilitate training and advice for all staff;
	• To liaise with the Local Authority and relevant agencies;
	• Is regularly updated in online safety issues and legislation, and be aware of the potential for serious child protection issues to arise from:
	  • sharing of personal data
	  • access to illegal / inappropriate materials
	  • inappropriate on-line contact with adults / strangers
	  • potential or actual incidents of grooming
	  • online bullying and use of social media.

Governors	• To ensure that the school follows all current online safety advice to keep the children and staff safe; • To be aware of online safety issues and support the head teacher in the development of the online safety policy; • To support the school in encouraging parents and the wider community to become engaged in online safety activities.
IT Manager (Camden's Schools IT team)	• To report any online safety related issues that arise, to the online safety coordinator; • To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed; • To ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date); • To ensure the security of the school IT system; • To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned

Role	Key Responsibilities
	devices; • To apply and update the school's policy on web filtering on a regular basis; • To inform the LGfL of issues relating to the filtering applied by the Grid; • To keep up to date with the school's Online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant; • To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster; • To keep up-to-date documentation of the school's online security and technical procedures
Teachers	• To embed online safety issues in all aspects of the curriculum and other school activities; • To adhere to the school's online safety policy and procedures; • To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant) • To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws; •
All school staff	• To read, understand and help promote the school's online safety policies and guidance; • To read, understand and adhere to the school staff Acceptable Use Agreement / Policy; • To report breaches of internet use to the online safety contact officer; • To recognise when pupils are at risk from their internet use or have had negative experiences and taking appropriate action, for example referral to the online safety contact officer. • To be aware of online safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices; • To report any suspected misuse or problem to the online safety coordinator; • To maintain an awareness of current online safety issues and guidance e.g. through CPD; • To model safe, responsible and professional behaviours in their own use of technology; • To ensure that any digital communications with pupils should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.

Role	Key Responsibilities
Pupils	• Read, understand and adhere to the Student / Pupil Acceptable Use Policy (NB: at KS1 it would be expected that parents / carers would sign on behalf of the pupils); • To have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations; • To understand the importance of reporting abuse, misuse or access to inappropriate materials; • To know what action to take if they or someone they know feels worried or vulnerable when using online technology; • To know and understand school policy on the use of mobile phones, digital cameras and hand held devices; • To know and understand school policy on the taking / use of images and on cyber-bullying; • To understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school, if related to their membership of the school.
Parents/carers	• To support the school in promoting online safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the Internet and the school's use of photographic and video images; • To read, understand and promote the school Pupil Acceptable Use Agreement with their children; • To consult with the school if they have any concerns about their children's use of technology.
External groups	• Any external individual / organisation will sign an Acceptable Use Policy prior to using any equipment or the Internet within school.

1.3 Communication

The policy will be communicated to staff/ pupils /parents and carers in the following ways:

- policy to be posted on the school website, in teaching computing curriculum folders and in the staffroom.
- staff are expected to sign an acceptable use agreement on appointment and this will be integrated into their general terms employment.
- acceptable use agreements discussed with pupils at the start of each year.
- acceptable use agreements to be issued to all parents /carers on entry to the school.
- acceptable use agreements to be held in pupil and personnel files.

2 Education and curriculum

2.1 Definition and purpose

Online 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.

Online 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.

An online safety curriculum enables schools to create a safe online 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 Pupil online safety curriculum

Our school is enabling an “online-safe” environment for pupils by ensuring that the following aspects are addressed. Our school has a clear, progressive online safety education programme as part of the computing and PHSE curriculum. This is built of the National Curriculum Computing Programme of Study.

This covers a range of skills and behaviours appropriate to their age and experience, including;

- to STOP and THINK before they CLICK;
- to develop a range of strategies to evaluate and verify information before accepting its accuracy;
- to be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
- to know how to narrow down or refine a search;
- [for older pupils] to understand how search engines work and to understand that this affects the results they see at the top of the listings;
- to understand acceptable behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
- to understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
- to understand why on-line ‘friends’ may not be who they say they are and to understand why they should be careful in online environments;
- to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings;
- to understand why they must not post pictures or videos of others without their permission;
- to know not to download any files – such as music files - without permission;
- to have strategies for dealing with receipt of inappropriate materials;

- to understand the impact of online bullying, sexting, extremism and trolling and know how to seek help if they are affected by any form of online bullying.
- to know how to report any abuse including online bullying; and how to seek help if they experience problems when using the Internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as ChildLine or the CLICK CEOP button.

2.3 Delivering online safety messages

The online safety contact officer is responsible for ensuring that all staff have the knowledge and resources to enable them to do so.

One of the key features of the school's online 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 online safety education lies with the associate head teacher and the online safety contact officer, but all teaching staff play an important role in delivering online safety messages. Teaching staff

- Plans Internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Will remind students about their responsibilities through an end-user Acceptable Use Policy which every student will sign/will be displayed throughout the school/will be displayed when a student logs on to the school network.
- Ensures staff will model safe and responsible behaviour in their own use of technology during lessons.
- Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright / intellectual property rights;
- Teachers should ensure that the school's policy on pupils' use of their own mobile phones in school is adhered to
- Ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying online; online gaming / gambling.

2.4 Pupils with Special Educational Needs

Pupils with learning difficulties or disability may be more vulnerable to risk from use of the internet and will require additional guidance on online safety practice as well as closer supervision.

Teachers are aware of those children who may be more vulnerable to risk from internet use, generally those children with a high level of experience and good computer skills but coupled with poor social skills.

SEN co-ordinators are responsible for providing extra support for these pupils and should:

- link with the online safety contact officer to discuss and agree whether the mainstream safeguarding systems on the internet are adequate for pupils with special needs;
- where necessary, liaise with the online safety contact officer and the Schools IT team to discuss any requirements for further safeguards to tailored resources and materials in order to meet the needs of pupils with special needs;
- ensure that the school's online safety policy is adapted to suit the needs of pupils with special needs;
- liaise with parents, carers and other relevant agencies in developing safety practices for pupils with special needs.
- keep up to date with any developments regarding emerging technologies and online safety and how these may impact on pupils with special needs.

2.5 Staff and governor training

This school

- Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection;
- Makes regular training available to staff on online safety issues and the school's online safety education program;
- Provides, as part of the induction process, all new staff (including those on university/college placement and work experience) with information and guidance on the online safeguarding policy and the school's Acceptable Use Policies.

2.6 Parent awareness and training

This school runs a rolling programme of advice, guidance and training for parents, including:

- introduction of the Acceptable Use Agreements to new parents, to ensure that principles of online safe behaviour are made clear;
- information leaflets; in school newsletters; on the school web site;
- demonstrations, practical sessions held at school;
- suggestions for safe Internet use at home;
- provision of information about national support sites for parents.

3 Online Safety Policies

3.1 Accessing and monitoring the system

- Access to LGfL (London Grid for Learning) at in our school is via an individual log-in and password. Children are reminded to keep this information in a safe and secure place.
- The online safety contact officer keeps a record of all log-ins used within the school for the purposes of monitoring and auditing internet activity.

- Network and technical staff responsible for monitoring systems are supervised by a senior member of their management team.
- Supervising teachers should be aware of what the children are doing at all times to allow an appropriate level of supervision of pupils.
- ICT lessons are planned carefully by the teacher before the lesson. Children should never be left to do 'free research' on the internet. They should use Espresso or follow clear and specific links prepared before the lesson. Children are taught how to search for information efficiently.
- Teachers or Support Staff need to be very clear with the children about which websites they are working on. The children should know what to do if they inadvertently go on a different website, that is, they put their hand up and tell the teacher immediately.

3.2 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 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 LGfL 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 not lend 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.

3.3 Safe use of ICT

3.3.1 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.
- All children at our school must 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.
- 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 online safety contact officer, who will liaise with the Schools IT team for temporary access. Teachers should notify the online safety contact officer once access is no longer needed to ensure the site is blocked.

3.3.2 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 year 5 and year 6 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.

In addition, year 6 pupils are taught the importance of respecting copyright and correctly quoting sources and told that plagiarism (copying others' work without giving due acknowledgement) is against the rules of the school.

3.3.3 Emails

- Children use the '2Simple' software '2-E-mail' which is a safe and secure way of learning to send e-mails. This software works solely within the class, with correspondence between the class teacher and the children only.
- Where teachers wish to add an external email address, this must be for a clear educational purpose and must be discussed with the online safety contact officer 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. Access to email systems by pupils is via a class email address only which the class teacher manages.
- All email messages sent by pupils in connection with school business must be checked and cleared by the responsible teacher.
- Apart from the associate headteacher, individual email addresses for staff or pupils should not be published on the school website.
- Pupils should be taught to be wary of opening attachments to emails where they are unsure of the content or have no knowledge of the sender.

3.3.4 Social networking sites, newsgroups and forums

- Social networking sites are blocked to pupils at our school.
- In order to teach pupils to stay safe on social networking sites outside of school, as part of online safety lessons, Key Stage 2 children are advised:
    - not to give out personal details to anyone on-line that may help to identify or locate them
    - anyone else, for example home address, name of school or clubs attended;
    - not to upload personal photos of themselves or others onto sites and to take care regarding what information is posted;
    - how to set up security and privacy settings on sites or use a "buddy list" to block unwanted communications or deny access to those unknown to them;
    - 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.

3.4.5 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.

Although children are not allowed to access these at school, pupils may use these at home.

- In order to teach pupils to stay safe whilst using chat rooms outside of school, they should be 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 online;
    - 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.

3.3.6 Video conferencing

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

- 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 network manager and should never enable individual pupils' names or other identifying information to be disclosed.

3.3.7 School website

- Content should not be uploaded onto the school website unless it has been authorised by the online safety contact officer and the head teacher, who are responsible for ensuring that content is accurate, suitable for the purpose and audience, and does not breach copyright or intellectual property law.
- The designated named people who have responsibility for uploading materials onto the website are: Greg Donohue and the school office.
- 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.

3.3.8 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 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 name.

3.5.9 Pupils' own mobile phone/handheld systems

The majority of pupils are likely to have mobile phones or other equipment that allows them to access internet services, and these can pose a major problem for schools in that they may be used for cyber bullying.

Year 5 and 6 pupils are permitted to bring mobile phones to school, however these are locked away in the school office during the school day.

4 Responding to incidents

4.1 Policy statement

- All incidents and complaints relating to online safety and unacceptable internet use will be reported to the online safety contact officer in the first instance. All incidents, whether involving pupils or staff, must be recorded by the online safety contact officer on the online safety incident report form.
- A copy of the incident record should be emailed to Camden's designated online 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 associate headteacher for action. Incidents involving the Headteacher should be reported to the chair of the board of governors.
- The school's online safety contact officer should keep a log of all online safety incidents and complaints and regularly review the information for evidence of emerging patterns of individual behaviour or weaknesses in the school's online safety system, and use these to update the online safety policy.
- Online safety incidents involving safeguarding issues, for example contact with inappropriate adults, should be reported to the designated child protection teacher, 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 online safety strategies and polices 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 online 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 online safety message and to demonstrate the school's "no blame" approach.
- The incident should be reported to the online safety contact officer and details of the website address and URL provided.
- The online safety contact officer should liaise with the network manager or Schools IT team to ensure that access to the site is blocked and the school's filtering system reviewed to ensure it remains appropriate.
- It is essential that teachers ensure that where they have an asked for filtering to be lifted for a particular lesson (eg: sex education) that they notify the Schools IT team so that filtering can be put back to minimise the risk of inappropriate sites being accessed by pupils or staff.

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.
- The incident should be reported to the online safety contact officer and details of the website address and URL recorded.
- The online safety contact officer should liaise with the network manager or Schools IT team to ensure that access to the site is blocked.
- The pupil's parents should be notified of the incident and the action to 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 headteacher and the online safety contact officer immediately.
- The online safety contact officer should notify the network manager 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 online safety incident report form.
- The online safety contact officer should arrange with the network manager or 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 headteacher 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 headteacher should report the incident to the police and follow their advice, which should also be recorded on the online 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 the school, whether or not they take place on school premises or outside school.

- School anti-bullying and behaviour policies and acceptable use policies should 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 online safety contact officer who will notify 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 should 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 online safety awareness and education, pupils should be 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

- Headteachers should be aware that teachers may become victims of cyber bullying by pupils. Because of the duty of care owed to staff, Headteachers should 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 online safety contact officer 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 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 head teacher 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 the online safety contact officer and the 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 online 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 online safety contact officer 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 online safety contact officer should make a note of all actions taken and contact the network manager or 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 online safety contact officer and the designated child protection teacher 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

Individual schools are responsible for deciding what sanctions will be applied for breach of acceptable ICT use policies. Sanctions applied should reflect the seriousness of the breach and should take into account all other relevant factors. The following is a framework recommended by LGfL that schools may want to adopt: For each point, schools may record their own detailed list of breaches and corresponding sanctions.

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.

Sanctions: referral to the class teacher as well as a referral to the online safety contact officer.

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 online 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.

Sanctions:
- referral to class teacher or tutor;
- referral to online safety contact officer;
- loss of internet access for a period of time;
- contacting parents.

5.1.3 Category C infringements

These are deliberate actions that 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 or pornographic material;
- purchasing or ordering items over the internet;
- transmission of commercial or advertising material.

Sanctions:

- referral to class teacher or tutor;
- referral to online safety contact officer;
- referral to Head of School ;
- any sanctions agreed under other school policies.

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 materials 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.

Sanctions:

- referral to Head of School;
- contact with parents;
- possible exclusion;
- removal of equipment;
- referral to community police officer;
- referral to Camden's online safety officer.

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 of School .

- excessive use of internet for personal activities not connected to professional development.
- use of personal data storage media (e.g. 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.

Sanctions: referral to the headteacher who will issue a warning.

5.2.2 Category B infringements

These infringements involve deliberate actions that call into question the person's suitability to work with children. They represent gross misconduct that would require a strong response and possible referral to other agencies such as the police or Safeguarding and Social Care.

- 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
- bringing the school name into disrepute.

Sanctions:

- referral to the Head of School;
- removal of equipment;
- referral to Camden's online safety officer;
- referral to SSC or police;
- suspension pending investigation;
- disciplinary action in line with school policies

Approval Date and Review:
Approved: November 2015
Date for review: November 2016

Appendix 1:
Acceptable use policy for 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 nasty message;
- not reply to any nasty 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 Fronter. 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 clearly identify my child and that their name will not be published.

Signed:

Date:

Appendix 2
Acceptable use policy for 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 online safety rules and the terms of this acceptable use policy. Failure to do so may result in disciplinary action being taken.
- Staff should only take pictures of children on school cameras and these should only be downloaded on to the school system (no pictures on personal cameras or mobile phones).
- 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 to report all online safety concerns to the online safety contact officer or Head of School
- 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 approved internet sites. The use of chat rooms or social networking sites 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 school USB sticks to transport data. Encrypted memory sticks will be provided to each teacher, these remain the property of the school and must be returned to the school on leaving.
- 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 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.

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

Name: _____

School: _____

Signed: _____

Date: _____

Appendix 3:
Online safety incident report form
This form should be kept on file and a copy emailed to Camden's online safety officer at jenni.spencer@camden.gov.uk

Name of school/organisation:
St Mary's CE Primary School
Address: Quex Road, London NW6 4PG
Name of online safety contact officer: Zoe Humphrey
Contact details: z.humphrey@stmarykilburn.camden.sch.uk

Details of incident
Date happened:
Time:
Name of person reporting incident:
If not reported, how was the incident identified?

Where did the incident occur?
□ 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, sexist, homophobic religious hate material
□ terrorist material
□ drug/bomb making material
□ child abuse images
□ on-line gambling
□ soft core pornographic material
□ illegal hard core pornographic material
□ 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

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 of School
□ advice sought from Safeguarding and Social Care
□ referral made to Safeguarding and Social Care
□ incident reported to police
□ incident reported to Internet Watch Foundation
□ incident reported to IT
□ disciplinary action to be taken
□ online safety policy to be reviewed/amended

Please detail any specific action taken (ie: removal of equipment)
Child/young person
□ incident reported to Head of School
□ 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 IT
□ child's parents informed
□ disciplinary action to be taken
□ child/young person debriefed
□ online safety policy to be reviewed/amended

Outcome of incident/investigation

Appendix 4:
Description of ICT applications

	Benefits	**Risks**
Internet	• Enables the storage, publication and retrieval of a vast range of information. • Supports communications 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 schools 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 communications over the network and the ability to attach documents. • Enables exchange of information and ideas and supports collaborative working. • Enhances written communications skills. • A good form of communication for children with some disabilities.	• Difficulties controlling contacts and content. • Use as a platform for bullying and harassment. • Risks from unwanted spam mail, particularly for fraudulent purposes or to introduce viruses to systems. • Hacking. • Unsolicited mail.
Chat/instant messaging	• Chat rooms allow users to chat on-line in real time in virtual meeting places with a number of people; • Instant messaging allows real-time chat for 2 people privately with no-one else able to join. Users have control over who they contact through “buddy lists”. • Enhances social development by allowing children to exchange experiences and ideas and	• Anonymity means that children are not aware of who they are really talking to. • Chat rooms may be used by predatory adults to contact, groom and abuse children on- line. • Risk of children giving away personal information that may identify or locate them. • May be used as a platform to bully or harass.

	form friendships with peers. • Use of pseudonyms protects the child's identity. • Moderated chat rooms can offer some protection to children. •	
Social networking sites	• On-line communities, including blogs and podcasts, where users can share text, photos and music with others by posting items onto the site and through messaging. • It allows creation of individual profiles. • Users can develop friends lists to allow access to individual profiles and invite comment. • Allows children to network with peers and join forums to exchange ideas and resources. • It provides a creative outlet and improves ICT skills.	• Open access means children are at risk of unsuitable contact. • Risk of children posting unsuitable material on-line that may be manipulated to cause them embarrassment or distress. • Children may post personal information that allows them to be contacted or located. • May be used as a platform to bully or harass.
File sharing (peer-to-peer networking)	• Allows users to share computer capability, networks and file storage. • Used to share music, video and other materials. • Allows children to network within a community of peers with similar interests and exchange materials.	• Illegal download and 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 violent crime due to theft. • Risk of cyberbullying via mobile phones.