E-SAFETY POLICY

Reviewed June 2018

Contents

1 Information on internet technology

1.1 Mission Statement & Introduction

At Emmanuel school broad opportunities are provided for individuals to develop their full potential and allow them to be healthy, happy and secure.

Building on our Christian ethos and in partnership with the whole school community, we provide a stimulating and caring environment where individuals are valued and nurtured morally, spiritually and academically. We stress the fundamental principle;

"Always treat others as you would like them to treat you" Matthew 7:12

It is commonly acknowledged that the educational and social benefits for children in using the internet should be promoted, but that this should be balanced against the need to safeguard children against the inherent risks from internet technology. Further, schools need to be able to teach children to keep themselves safe whilst on-line.

This document provides schools with guidance on developing an effective e-safety strategy to enable these aims to be achieved and support staff to recognise the risks and take action to help children use the internet safely and responsibly.

1.2 Benefits and risks

Computing covers a wide range of activities, including access to information, electronic communications and social networking. The table shown at appendix 5 provides brief details of the various uses of the internet together with their benefits and risks.

As use of technology is now universal, it is imperative that children learn computing skills in order to prepare themselves for the working environment and that the inherent risks are not used to reduce children's use of technology. Further, the educational advantages of computing need to be harnessed to enhance children's learning.

The risk associated with use of technology by children can be grouped into 4 categories.

1.2.1 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 such as pornography, or information advocating violence, racism, suicide or illegal and anti-social behaviour that they are unable to evaluate in a critical manner.

1.2.2 Contact

Chat rooms, gaming sites 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 sexually abusing 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.

1.2.3 Commerce

Children are vulnerable to unregulated commercial activity on the internet that could have serious financial consequences, such as fraud or identity theft, 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. Contact via social networking sites can also be used to persuade children to reveal computer passwords or other information about the family for the purposes of fraud.

1.2.4 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 Purpose and description

Computing is now a key part of our school curriculum and one of the key aims of computing is to ensure that pupils are aware of e-safety messages. This is part of our school's responsibility to safeguard and promote the welfare of pupils, as well as the duty of care to children and their parents to provide a safe learning environment.

We have an e-safety strategy in place based on a framework of policy, practice, education and technological support that ensures a safe e-learning environment that maximises the educational benefits of ICT whilst minimising the associated risks. Its purpose is to:

- promote the use of technology within the curriculum
- protect children from harm
- safeguard staff in their contact with pupils and their own use of the internet
- ensure the school fulfils its duty of care to pupils
- provide clear expectations for staff and pupils on acceptable use of the internet.

In particular, we ensure the following:

- A ***safe internet platform*** that provides filtering software to block access to unsuitable sites, anti-virus software and monitoring systems (for example the London Grid for Learning platform).

- A culture of ***safe practice*** underpinned by a strong framework of e-safety policy that ensures everyone is aware of expected standards of on-line behaviour.

- Children are ***taught to keep themselves and others safe*** on-line and use technology responsibly; this should be achieved by working in partnership with parents and carers and raising awareness of the potential risks of internet use.

2.2   Roles and responsibilities

A successful e-safety strategy needs to be inclusive of the whole school community, including teaching assistants, governors and others, and forge links with parents and carers. The strategy has the backing of school governors, and is overseen by the Headteacher and is fully implemented by all staff, including technical and non-teaching staff.

2.2.1 Headteacher's role

Headteachers have ultimate responsibility for e-safety issues within the school 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
- ensuring e-safety is embedded in the curriculum
- deciding on sanctions against staff and pupils who are in breach of acceptable use policies.

2.2.2 Governors' role

Governing bodies have a statutory responsibility for pupil safety and should therefore be aware of e-safety issues, providing support to the Headteacher in the development of the school's e-safety strategy.

Governors are subject to the same e-safety rules as staff members and sign an Acceptable Use Agreement in order to keep them safe from allegations and ensure a high standard of professional conduct. In particular, governors should always use business email addresses when conducting school business.

2.2.3 E-safety contact officer's role

Emmanuel School has a designated e-safety contact officer who is responsible for co-ordinating e-safety policies on behalf of the school. The Headteacher is the school's Designated Child Protection and Safeguarding Lead and the E-Safety Contact Officer.

The e-safety contact officer has the authority, knowledge and experience to carry out the following:

- 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 computing leader to ensure they are kept up to date with e-safety issues and to advise of any new trends, incidents and arising problems to the Headteacher
- assess the impact and risk of emerging technology and the school's response to this in association with IT staff and learning platform providers
- raise the profile of e-safety awareness with 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
- maintain a log of internet related incidents and co-ordinate any investigation into breaches
- report all incidents and issues to Camden's e-safety officer.

In addition, the e-safety contact officer receives recognised training CEOP or E-PICT in order to carry out their role more effectively.

2.2.4 IT manager's role

At Emmanuel, this function is carried out by the Camden's School IT Team:

- the maintenance and monitoring of the school internet system including 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.

2.2.5 Role of school staff

All school staff have a dual role concerning their own internet use and providing guidance, support and supervision for pupils. Their role is:

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

2.2.6 Designated safeguarding lead

Where any e-safety incident has serious implications for the child's safety or well-being, the matter should be referred to the designated child protection person for the school who will decide whether or not a referral should be made to Family Services and Social Work or the Police.

2.3 Pupils with special needs

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

Our Inclusion Leader is responsible for providing extra support for these pupils and should:

- link with the e-safety contact officer to discuss and agree whether the mainstream safeguarding systems on the internet are adequate for pupils with special need
- where necessary, liaise with the e-safety contact officer and the IT service to discuss any requirements for further safeguards to the school IT system or tailored resources and materials in order to meet the needs of pupils with special needs
- ensure that the school'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.

2.4   Working with parents and carers

It is essential for Emmanuel School to involve parents and carers in the development and implementation of e-safety strategies and policies; most children will have internet access at home or own mobile devices 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.

Annual e-safety workshops for parents are put in place in order to ensure parents are aware of e-safety issues and support them in reinforcing e-safety messages at home.

Parents are provided with information on computing and the school's e-safety policy – available on school website and when they are asked to sign acceptable use agreements on behalf of their child so that they 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 school internet system is via individual log-ins and passwords for staff and pupils wherever possible. Visitors should have permission from the Headteacher to access the system and be given a separate visitors log-in.

- The e-safety contact officer and teaching staff should carefully consider the location of internet enabled devices in classrooms and teaching areas in order to allow an appropriate level of supervision of pupils depending on their age and experience.

3.2   Confidentiality and data protection

- The school will ensure that all data held on its IT systems is held in accordance with the principles of the Data Protection Act 2018. Data will be held securely and password protected with access given only to staff members on a "need to know" basis.

- Pupil data that is being sent to other organisations will be encrypted and sent via a safe and secure system. Any breaches of data security should be reported to the head teacher immediately.

- Where the school uses CCTV, a notice will be displayed in a prominent place to ensure staff and students are aware of this and recordings will not be revealed without appropriate permission.

3.3 Acceptable use policies

- All internet users within the school will be expected to sign an acceptable use agreement that sets out their rights and responsibilities and incorporates the school e-safety rules regarding their internet use.

- For Emmanuel pupils, acceptable use agreements will be signed by parents on their child's behalf at the same time that they give consent for their child to have access to the internet 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).

The e-safety contact officer will keep a copy of all signed acceptable use agreements.

3.4 Teaching e-safety

3.4.1 Responsibility

One of the key features of the school'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 Headteacher but all staff should play a role in delivering e-safety messages.

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

- Teachers are primarily responsible for delivering an ongoing e-safety education in the classroom as part of the curriculum.

- Rules regarding safe internet use should be 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 be 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.

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

3.4.2 Content

Pupils should be taught all elements of e-safety included in the computing curriculum so that they:

- use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

- can evaluate and apply information technology, including new or unfamiliar technologies, analytically to solve problems

- are responsible, competent, confident and creative users of information and communication technology.

3.5 IT 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. Staff should refer to the Social Media Policy for school staff for further guidance.

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.

- 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 the school email system 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.

- When making contact with parents or pupils by email, staff should always use their school email address or account. Personal email addresses and accounts should never be used.

- 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 or i-pads provided by the school, they should ensure that the equipment is kept safe and secure at all times.

3.5.2 Exit strategy

When staff leave, their line manager should liaise with the network manager to ensure that any school equipment is handed over and that PIN numbers, passwords and other access codes to be reset so that the staff member can be removed from the school's IT system.

3.6 Safe use of technology

3.6.1 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 Emmanuel all children will 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 e-safety contact officer, who will liaise with the IT service provider for temporary access. Teachers should notify the e-safety contact officer once access is no longer needed to ensure the site is blocked.

3.6.2 Evaluating and using internet content

Teachers should teach pupils good research skills that help them to maximise the resources available on the internet so that they can use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content.

3.6.3 Safe use of applications

School email systems is hosted by an email system that allows content to be filtered and allow pupils to send emails to others within the school or to approved email addresses externally.

Social networking sites such as Facebook, MySpace and Twitter allow users to publish information about them to be seen by anyone who has access to the site. These are not used in our school but pupils are likely to use these sites at home.

Newsgroups and forums are sites that enable users to discuss issues and share ideas on-line. These are not used in our school.

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 school internet systems do host these applications.

Gaming-based sites allow children to "chat" to other gamers during the course of gaming. Many of the gaming sites are not properly moderated and may be targeted by adults who pose a risk to children. Consequently such sites should not be accessible via school internet systems

Safety rules

- Access to and use of personal email accounts, unregulated public social networking sites, newsgroups or forums, chat rooms or gaming sites on the school internet system is forbidden and should be blocked.

- If schools identify a clear educational use for emails or social networking sites and forums for on-line publishing, they should only use approved sites such as those provided by the IT service provider. Any use of these sites should be strictly supervised by the responsible teacher.

- Emails should only be sent via the school internet system to addresses within the school system or approved external address. All email messages sent by pupils in connection with school business must be checked and cleared by the responsible teacher.

- 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 officer who will liaise with the learning platform provider.

- 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.

- Pupils should be taught not to disclose personal contact details for themselves or others such as addresses or telephone numbers via email correspondence or on social networking sites.

- All electronic communications should be polite; if a pupil receives an offensive or distressing email or comment, 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, chat rooms or social networking sites will not be tolerated and will be dealt with in accordance with the school's anti-bullying policy. This should include any correspondence or contact taking place outside the school and/or using non-school systems or equipment.

- Users should be aware that as use of the school internet system is for the purposes of education or school business only, and its use may be monitored.

- In order to teach pupils to stay safe online outside of school, they should be 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 to only use moderated chat rooms that require registration and are specifically for their age group

- not to upload personal photos of themselves or others onto sites and to take care regarding what information is posted as there is no control where images may end up or who can see 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
- not to give out personal details to anyone on-line that may help to identify or locate them or anyone else
- not to arrange to meet anyone whom they have only met on-line or go "off-line" with anyone they meet in a chat room
- 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.

3.6.4 Video conferencing (where appropriate)

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

- Teachers will try to use a safe video conferencing platform, ie: London Grid for Learning and need to be aware of the risks associated with live video feeds.

- 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.

3.6.5 School website

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

- Members of the School Leadership Team 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 will be contained on the website.

- Children's full names, alongside a photograph, 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.

3.6.6 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.

- 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 name and all images held of children should be deleted once the child has left the school.

- Staff should not use personal devices to take photographs of pupils.

- Schools should inform parents that although they may take photographic images of school events that include other children, it is on the understanding that these images are for personal use only and will not be published on the internet or social networking sites.

3.6.7 Pupils own mobile phone/handheld systems

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

Emmanuel school does not allow children to use their mobile devices during school hours. Children with mobile phones hand them to the class teacher at the stat of the day and collect them at the end of the day.

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 officer in the first instance. All incidents, whether involving pupils or staff, must be recorded by the e-safety contact officer 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 Headteacher for action and consideration given to contacting the LADO (*Local Authority Designated Officer)* where this is appropriate. Incidents involving the headteacher should be reported to the chair of the board of governors.

- The school's e-safety contact officer 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 Person, who will make a decision as to whether or not to refer the matter to the police and/or Family Services and Social Work.

Although it is intended that e-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 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 officer and details of the website address and URL provided.

- The e-safety contact officer should liaise with the network manager or learning platform provider 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 officer and details of the website address and URL recorded.

- The e-safety contact officer should liaise with the network manager or learning platform provider 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 IT by staff

- If a member of staff witnesses misuse of IT by a colleague, they should report this to the Headteacher immediately. If the misconduct involves the Headteacher or governor, the matter should be reported to the chair of the board of governors.

- The e-safety contact officer will notify the network manager so that the computer, laptop or other device 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 officer will arrange with the network manager or learning platform provider 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 will take any necessary disciplinary action against the staff member and report the matter to the school governors and the police where appropriate. Where appropriate, consideration should be given to contacting the LADO for advice.

- If the materials viewed are illegal in nature the head teacher or governor 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   Cyberbullying

4.5.1   Definition and description

Cyberbullying is defined as the use of technology such as email and social networking sites to deliberately hurt or upset someone or harass or threaten. 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 images or videos of someone via mobile phone or email (for example, sexting/"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 e-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 e-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 send or post inappropriate images of themselves
  - 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.

Any action taken on cyber bullying incidents must be proportional to the harm caused. For some cases, it may be more appropriate to help the pupils involved to resolve the issues themselves rather than impose sanctions.

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 communications. 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. 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. The pupil should also consider changing email address.

- Where bullying takes place in chat rooms or gaming sites, the pupil should leave the chat room or gaming site 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 Cyberbullying of teachers

- Headteachers should be aware that teachers may become victims of cyberbullying 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 cyberbullying of teachers should be incorporated into any anti-bullying policies, education programme or discussion with pupils so that they are aware of their own responsibilities.

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

- Teachers should follow the guidance on safe IT 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 cyberbullying of pupils and not reply to messages but report the incident to the Headteacher immediately.

4.6   Sexting and sexual abuse and harassment by peers

The internet contains a high level of sexually explicit content and internet-based communications systems and social networking sites can be used to send sexually explicit messages and images. In some cases these actions may be harmful or abusive or may constitute harassment or online bullying.

"Sexting" or the sending of sexual images between young people via the internet or mobile devices is a particular issue young people need to know that producing and sharing these images is illegal. Pupils need to understand that once the image is sent, they have lost control of who it is distributed to and how it is used, and that there is a good chance that the image will be widely seen, possibly including parents.

Staff need to be able to react to incidents in a proportional manner so that the welfare of young people is safeguarded and no young person is unnecessarily criminalised. Guidance for responding to incidents is available at:
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/551575/6.2439_KG_NCA_Sexting_in_Schools_WEB__1_.PDF

Schools need to be aware of the use of IT by older pupils for the purpose of distributing unsuitable materials and sexually harassing other pupils and be able to safeguard pupils from this. Schools should be aware of the duty under statutory guidance *Keeping children safe in education* and *Sexual violence and sexual harassment between children in schools and colleges* which requires schools to have policies in place to deal with incidents of on-line sexual harassment. Schools should refer to the CSCB *Sexually harmful behaviour protocol* for further details. https://cscb-new.co.uk/?page_id=8266

Schools should also be aware of when any of these behaviours may be linked to the sexual exploitation of a pupil or is being carried out as a gang-related activity. Staff should refer to the CSCB child sexual exploitation guidance for further details. http://www.cscb-new.co.uk/wp content/uploads/2015/09/Multi_Agency_Guidance_On_Child_Sexual_Exploit tion_2015.pdf

4.7 Risk from inappropriate contacts with adults

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 Designated Child Protection Person who is also the e-safety contact officer.

- The Designated Child Protection Person 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 Family Services and Social Work 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 Person can seek advice on possible courses of action from Camden's e-safety officer in Family Services and Social Work.

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

- The Designated Child Protection Person 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 IT equipment or networks, the e-safety contact officer should make a note of all actions taken and contact the network manager or learning platform provider 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.

4.8   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 officer/Designated Child Protection Person 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.

- Where there are concerns that a young person is being radicalised or is in contact with violent extremists, or that their parents are and this is placing the child or young person at risk, schools should refer the young person to the Channel Co-ordinator for support.

4.9   Risk from sites advocating suicide, self-harm and anorexia

Some internet sites advocate dangerous activities such as self-harming, suicide or anorexia. Other sites contain sexually explicit material or glorify risky and illegal behaviours like substance misuse.

Exposure to potentially harmful materials online may normalise the issue for young people and desensitise them to the harm. Most young people who visit these sites will not be adversely affected, but some vulnerable, less resilient young people may feel drawn to the sites which may trigger harmful or even fatal behaviours.

- *The school should ensure that young people have an opportunity to openly discuss issues such as self-harming, suicide, substance misuse and anorexia as part of the PHSE curriculum.*
- *Pastoral support should be made available to all young people to discuss issues affecting them and to establish whether their online activities are an added risk factor*
- *Staff should receive the training needed to raise awareness of these issues so that they are able to identify those young people who are at risk, offer appropriate support and make appropriate referrals for help.*

5   Sanctions for misuse of school IT

Sanctions will be applied for breach of Acceptable Use Policies. Sanctions applied should reflect the seriousness of the breach and should take into account all other relevant factors. Emmanuel School adopted a framework recommended by LGfL.

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 could include meeting with the class teacher as well as a referral to the e-safety contact officer, missing minutes of their playtime/lunchtime. A child will be given a warning & moved to 'Amber' on the class behaviour traffic lights.

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 or prohibited sites during lessons
- continued unauthorised use of email, mobile phones or social networking sites during lessons

- use of file sharing software
- accidentally corrupting or destroying other people's data without notifying staff
- accidentally accessing offensive material without notifying staff.

Sanctions could include:

- meeting with class teacher
- meeting with e-safety contact officer
- any sanctions agreed under behaviour school policy ie missing some playtime/lunchtime, named moved up on class behaviour traffic lights, missing some of golden time
- contacting parents

5.1.3 Category C infringements

These are deliberate actions that either negatively affect school ICT systems 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
- transmission of commercial or advertising material.

Sanctions could include:

- meeting with class teacher
- meeting with e-safety contact officer
- meeting with Headteacher
- contact with parents
- any sanctions agreed under the behaviour policy – missing most of playtime/lunchtime, named moved to 'Red' on class behaviour traffic lights, missing most of golden time

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 could include:

- referral to head teacher
- contact with parents
- possible exclusion
- removal of equipment
- referral to community police officer
- referral to Camden's e-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 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 and social media sites such as Twitter/Facebook 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.

Possible sanctions include referral to the head teacher who will issue a warning.

5.2.2 Category B infringements

These infringements involve deliberate actions that undermine safety on the internet and activities 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 Camden's LADO.

- 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.

Possible sanctions include:
- referral to the head teacher
- removal of equipment
- referral to Camden's e-safety officer
- referral to Camden's LADO or the police
- suspension pending investigation
- disciplinary action in line with school policies.

Policy reviewed   June 2018

Agreed review schedule   3 years

Next review due   June 2021

Reviewed by (signature)

Fr Jonathan Kester, Chair of FGB   Kathryn Fitzsimmons, Headteacher

(updated in November 2018)

ACCEPTABLE USE POLICY FOR EMMANUEL PRIMARY SCHOOL PUPILS	

Name:	
Year Group & Class:	

I want to stay safe while I am using a computer and/or mobile phone 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 or message 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 and mobile phone use and agree that my child may have access to the internet at school. 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 to monitor my child's internet usage and websites they access. I will be proactive in seeking advice from the school.

Signed:	
Date:	

ACCEPTABLE USE POLICY FOR EMMANUEL PRIMARY SCHOOL STAFF & GOVERNORS

Access and professional use

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

- Staff and governors 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 against staff or governors being removed.

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

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

- 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 and governors will have access to the internet as agreed by the school but will take care not to allow pupils to use their logon to search the internet.

Data protection and system security

- Staff and governors 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 such as USB sticks is permitted where virus checks can be implemented on the school ICT system using SOPHOS software.

- Downloading executable files or unapproved system utilities will not be allowed and all files held on the school ICT system 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 and governors should not browse, download or send material that could be considered offensive to colleagues and pupils or is illegal.

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

- School ICT systems may not be used for private purposes without permission from the head teacher.

- Use of school ICT systems for financial gain, gambling, political purposes or advertising is not permitted.

I understand that failure to comply with this agreement could lead to disciplinary action. I have read the above policy and agree to abide by its terms.

Signature .... Date ....

Full Name .... (printed)

Job title ....

School ....

Authorised Signature (Head Teacher)

I approve this user to be set-up.

Signature .... Date ....

Full Name .... (printed)

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/organisation's details:

Name of school/organisation:

Address:

Name of e-safety contact officer:

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?
□ 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 teacher/senior manager
☐ advice sought from Family Services and Social Work
☐ referral made to Family Services and Social Work
☐ incident reported to police
☐ incident reported to Internet Watch Foundation
☐ incident reported to IT
☐ 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/senior manager
☐ advice sought from Family Services and Social Work
☐ referral made to Family Services and Social Work
☐ 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
□ e-safety policy to be reviewed/amended

Outcome of incident/investigation