E-Safety Policy

New End Primary School

Date Reviewed: Spring Term 2019

Next Review Date: Spring Term 2020

Rationale

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

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

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

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

This document provides guidance to achieve this by helping to recognise the risks and take action to help children use the internet safely and responsibly.

Internet Technology

Internet technology provides a wide range of activities, including access to information, electronic communications and social networking; each has a clear educational use but also inherent risks for children.

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

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

- raising educational attainment, engaging and motivating pupils to learn and improving their confidence
- improving pupil's research and writing skills
- allowing children with disabilities to overcome communications barriers
- enabling children to be taught "remotely", for example children who are unable to attend school
- improving pupil's wellbeing through the social and communications opportunities offered
- providing access to a wide range of educational materials and teaching resources.

Risks associated with Internet Technology

The risk associated with use of ICT by children can be grouped into 4 categories – content, contact, commerce and culture.

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

Contact

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

Commerce

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

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.

School E-Safety Strategies

Definition and purpose of e-safety

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

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

An e-safety strategy enables schools to create a safe e-learning environment that:

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

Elements of e-safety

New End has enabled an "e-safe" environment for pupils by ensuring that the following aspects are addressed:

Safe systems

New End is connected to the Internet through the London Grid for Learning platform. This offers a safe e-learning environment by providing filtering software to block access to unsuitable sites, anti-virus software and internet monitoring systems. All pupils form Year 1 – Year 6 have access to online platforms Sumdog and Purple Mash in school and at home using a personal username and password. On these sites teachers set tasks for children to complete, though a range of games and/or tools. These sites are password protected. Sumdog only allows teachers to send messages to students. Purple Mash has a blog system which is monitored by teachers and all posts have to be approved by an adult before publication. Neither website has an instant chat/messaging service between students or permits messaging from members of the public, teachers or pupils from other schools.

Safe practices

Within school all staff are aware of the school rules on using technology to minimise risk to themselves and the children. They model safe practice on the internet at all time. Children are taught explicitly and implicitly about staying safe online.

Safety awareness

It is vital that children are able to keep themselves and others safe and use the internet responsibly. We aim to work in partnership with parents and carers, who have an important role in raising pupils' awareness of the potential dangers of using the internet and helping them to develop their own strategies to avoid these risks and keep safe on-line.

Because many children will have access to the internet at home, we offer advice and try to ensure that parents and carers are fully aware of e-safety issues so that they can extend e-safety strategies to the home environment. Where issues arise we work with the children and families to help educate and eliminate any risks posed.

Roles and Responsibilities

A successful e-safety strategy needs to be inclusive of the whole school community and forge links with parents and carers. We recognise that the strategy must have the backing of school governors, is overseen by the head teacher and is fully implemented by all staff, including technical and non-teaching staff.

The Headteacher has 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 and forward the school's e-safety strategy
- ensuring e-safety is embedded in the curriculum
- deciding on sanctions against staff and pupils who are in breach of acceptable use policies.

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

The e-safety contact officer is the headteacher who is responsible for co-ordinating e-safety policies on behalf of the school. 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 IT Manager to ensure they are kept up to date with e-safety issues and to advise of any new trends, incidents and arising problems to the head teacher
- assess the impact and risk of emerging technology and the school's response to this in association with IT staff and the Schools IT team
- 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.

The ICT Leader of Teaching and Learning together with Camden's Schools IT team ensure:

- the maintenance and monitoring of LGFL, 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.

Teaching 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 Fronter
- 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.

Where any e-safety incident has serious implications for the child's safety or well-being, the matter is referred to the designated child protection teacher for the school who decides whether or not a referral should be made to Safeguarding and Social Care or the Police. At New End the designated child protection teacher is the headteacher.

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 e-safety practice as well as closer supervision.

The SENDCo 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 Fronter are adequate for pupils with special need.
- where necessary, liaise with the e-safety contact officer and the Schools IT team to discuss any requirements for further safeguards to Fronter or tailored resources and materials in order to meet the needs of pupils with special needs
- ensure that the 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.

Working with Parents and Carers

Most children will have internet access at home and might not be as closely supervised in its use as they would be at school. Therefore, parents and carers need to know about the risks so that they are able to continue e-safety education at home and regulate and supervise children's use as appropriate to their age and understanding.

The headteacher, governors and the e-safety contact officer should consider what strategies to adopt in order to ensure parents are aware of e-safety issues and support them in reinforcing e-safety messages at home.

Parents should be provided with information on ICT learning and the school's e-safety policy 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.

Accessing and monitoring the system

Access to Sumdog and Purple Mash the school has signed up to is via an individual log-in and password

The ICT co-ordinator has 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 at Camden IT are supervised by a senior member of their management team

The location of computer terminals in classrooms and teaching areas in order to allow an appropriate level of supervision of pupils depending on their age and experience

Children do not have access to the computers/internet without supervision from an adult member of staff

Teaching e-safety

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 head teacher and the e-safety contact officer, but all teaching 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. This is done through staff training.

Pupils should be taught:

- the benefits and risks of using the internet
- how their behaviour can put themselves and others at risk
- what strategies they can use to keep themselves safe
- what to do if they are concerned about something they have seen or received via the internet
- who to contact to report concerns
- that the school has a "no blame" policy so that pupils are encouraged to report any e-safety incidents
- that the school has a "no tolerance" policy regarding cyber bullying
- behaviour that breaches acceptable use policies will be subject to sanctions and disciplinary action

- Mobile devices are not allowed during school hours – they should be handed to the office on arrival in school.

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

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 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.

ICT and safe teaching practice

School staff are 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 and only on school equipment
- 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 (most are blocked on the school filtering of the internet to minimize this risk).
- 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 via Sumdog or Purple Mash, 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
- Where staff are using mobile equipment such as laptops or iPads provided by the school, they should ensure that the equipment is kept safe and secure at all times.

Safe use of ICT

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.

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 ICT co-ordinator, who will liaise with the Schools IT team for temporary access. Teachers should notify the ICT Co-ordinator once access is no longer needed to ensure the site is blocked.

Emails

All children have a Google account to access the Chromebooks. Access to and use of personal email accounts through Gmail is forbidden and blocked. This is to protect pupils from receiving unsolicited mail and preserve the safety of the system from hacking and viruses.

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

Apart from the head teacher, 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.

Social networking sites, newsgroups and forums

Social networking sites such as Facebook, MySpace and Bebo allow users to publish information about them to be seen by anyone who has access to the site. Generally, these would have limited use in schools 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.

Access to unregulated public social networking sites, newsgroups or forums is blocked within school

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

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

- 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
- 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

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.

Access to public or unregulated chat rooms will be blocked.

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

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.

School website

Content should not be uploaded onto the school website unless it has been authorised by the e-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.

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.

Photographic and video images

The school will send out letters asking parents to inform the school if they do not wish photos of their children to be used on the web-site or in the local press.
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.

Pupils own mobile phones/handheld systems

Many parents prefer their children to have mobile phones with them in order to ensure their safety and enable them to contact home if they need to. **At New End, mobile phones must be handed into the office in the morning and will be handed back at the end of the day**

Responding to Incidents

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

Where the incident or complaint relates to a member of staff, the matter must always be referred to the head teacher for action. Incidents involving the 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 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 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.

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 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.

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 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 Schools IT team to ensure that access to the site is blocked.

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

Inappropriate use of ICT by staff

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

The e-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 e-safety incident report form.

The e-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 head teacher should take any necessary disciplinary action against the staff member and report the matter to the school governors and the police where appropriate.
If the materials viewed are illegal in nature the head teacher should report the incident to the police and follow their advice, which should also be recorded on the e-safety incident report form.

Cyber bullying

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. It 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.

School anti-bullying and behaviour policies and acceptable use policies covers 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 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.

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

Head teachers should be aware that teachers may become victims of cyber bullying by pupils. Because of the duty of care owed to staff, head teachers 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 e-safety contact officer in the same manner as incidents involving pupils. Teachers should follow the guidance on safe ICT use in 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.

Risks 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 e-safety contact officer and the designated child protection teacher.

The designated child protection teacher 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 teacher can seek advice on possible courses of action from Camden's e-safety officer in Safeguarding and Social Care.

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

The designated child protection teacher and the e-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 e-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

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 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.