

Keeping children safe on-line: Online safety policy and guidance for the children's workforce in Camden 2018

CONTENTS

	Page	
1.	Introduction	2
2.	Benefits and risks of IT	2
3.	Camden's online safety strategy	4
4.	Preventative work	5
5.	Dealing with specific risks	8
	 5.1 Cyberbullying 5.2 Inappropriate contacts and non-contact sexual abuse 5.3 Online child sexual exploitation 5.4 Contact with violent extremists 5.5 Websites advocating extreme or dangerous behaviours 	
6.	Responding to child protection incidents	13
7.	IT and safe working practice	17
Арр	endix 1: Online incident report form	19

1 Introduction

Internet technology (IT) is now an integral part of children's lives and 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 social development, 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 may not be aware of the actions they can take to protect them.

It is Camden'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. Camden has a council-wide online safety strategy designed to educate children and parents of the risks related to internet use and what steps to take to reduce risk and deal with arising issues.

Staff who work with children have a role in implementing this strategy by helping the children they work with to keep themselves safe on-line and dealing with safeguarding issues arising from online safety incidents.

This document provides guidance to staff on how to recognise the risks of internet use and take action to reduce these risks. The guidance also sets out what actions should be taken where a child's use of the internet puts them at risk of significant harm.

2 Benefits and risks

Internet technology allows children to access to information, electronic communications and social networking and can support their education and social development.

However, use of the internet can also carry inherent risks:

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 or illegal and antisocial 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 or sexual images that may be widely shared. 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.

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
- online bullying
- use of mobile devices to take and distribute inappropriate images of the young person (sexting) that cannot be removed from the internet and can be forwarded on to a much wider audience than the child intended.

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.

They may visit sites that advocate extreme and dangerous behaviour such as self-harm or suicide or violent extremism, and more vulnerable children may be at a high degree of risk from such sites. All children may become desensitised to pornography, violence, sex and drug use or self-harm by regularly viewing these on-line.

3 Camden's online safety strategy

3.1 Definition and purpose

Online safety contributes to the "staying safe" element of good outcomes for children and Camden has developed a borough-wide online safety strategy encompassing all services where children are able to access the internet.

The purpose of the strategy is to:

- protect children from harm
- safeguard staff in their contact with children and their own use of the internet
- ensure services fulfil the duty of care to children
- provide clear expectations for staff and children on acceptable use of the internet.

3.2 Elements of online safety

Under the strategy, services that provide internet access for children, such as schools, libraries and youth clubs must ensure a safe online environment for children by:

 ensuring safe systems through use of safe filtering to block access to unsuitable sites.

For example, most Camden schools are linked to the internet via a safe internet platform and libraries provide separate computers for children and adults with different filtering.

- monitoring children's access and use of IT
- providing safe practices through the use of online safety policies and acceptable use agreements that set out the users rights and responsibilities and sanctions for breach of these agreements
- promoting safety awareness and providing guidance and information so that children are taught how to keep themselves and others safe and use the internet responsibly
- working with parents and carers to ensure online safety messages are extended to the home environment.

3.3 Online safety contact officer

Every service should have a designated online safety contact officer who takes the lead for co-ordinating the development, implementation and review of online safety policies within the service.

All online safety incidents should be reported to the online safety officer who will decide what action needs to be taken to improve online safety practice and deal with individual incidents.

Where any online safety incident has serious implications for the child's safety or well-being, the online safety officer must discuss the matter with the designated safeguarding lead for the service who will decide whether or not a referral should be made to CSSW or the Police.

Each service's online safety officer should also report all incidents and issues to Camden's online safety officer who is based in the Children's Quality Assurance Unit of the Children's Safeguarding and Social Work division (CSSW). The form is shown at Appendix 1. This is to ensure that CSSW has oversight of any emerging safeguarding issues linked to internet use, which is particularly important given the rapid development of technologies.

4 Preventative work

Staff may have concerns about the internet use of a child with whom they work, and parents may express concerns themselves. It is important that staff are aware of the key risks and safety messages for children and parents in order to use the internet safely so that they can advise children and parents accordingly.

4.1 Key online safety messages

Children need to be guided on:

- 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 they won't be blamed if they report any online safety incidents
- that online bullying cannot be tolerated
- the basic principles of "netiquette" (how to behave on the internet).

Staff should be aware that some children may be more vulnerable to risk from internet use, generally those children with a high level of computer skills but coupled with poor social skills.

4.2 Safe use of ICT

- When using the internet and internet search engines, children should receive the appropriate level of supervision for their age and understanding. Search engines should have an appropriate level of filtering to block access to unsuitable sites.
- When using email, children should be taught:
 - o to keep messages polite
 - not to disclose personal contact details for themselves or others
 - to tell their parent or carer immediately if they receive an offensive or distressing email
 - o not to use email to bully or harass others
 - be wary of opening attachments to emails where they are unsure of the content or have no knowledge of the sender
- When using social networking sites such as Facebook or newsgroups and forum sites, children should be taught:
 - 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
 - be cautious about using "check in" facilities that show people's location

- 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.
- When using chat rooms or online gaming sites, children should be taught:
 - not to give out personal details to anyone on-line that may help to identify or locate them or anyone else
 - to only use moderated chat rooms that require registration and are specifically for their age group
 - o not to arrange to meet anyone whom they have only met on-line
 - to behave responsibly whilst on-line and keep communications polite
 - not to respond to any hurtful or distressing messages but to let their parents or carers know so that appropriate action can be taken
 - that any bullying or harassment via chat rooms or instant messaging may have serious consequences.
- When using web cameras, children should be taught:
 - o to use them only with people who are well known to them
 - not to do anything that makes them feel uncomfortable or embarrassed
 - to tell their parents or carers if anyone is trying to force them to do something they don't want to.

Staff who work with children who need help on keeping safe on the internet can provide them with a copy of Camden's "top safety tips" poster available from CSSW.

4.3 Children with special educational needs and disabilities (SEND)

Children with SEND may be more vulnerable to risk from use of the internet and may need additional guidance on online safety practice as well as closer supervision. Staff may wish to discuss this with parents and carers and help them to access information and resources from specialist agencies.

5 Dealing with specific risks

5.1 Online bullying

Online bullying is defined as the use of IT to deliberately hurt or upset someone. Unlike traditional 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.

Online bullying is extremely prevalent as children 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. In extreme cases, online bullying could be a criminal offence.

Bullying may take the form of:

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

Most incidents of online bullying will not necessarily reach significant harm thresholds and will probably be best dealt with the service's own anti-bullying or acceptable use policies with the co-operation of parents.

Children should be taught:

- not to disclose their password to anyone
- 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
- o not to respond to offensive messages
- o to tell their parents about any incidents immediately.

Parents and carers should be taught to be vigilant about possible online bullying and how to work with internet and mobile service providers to cut down on the risk of online bullying:

- mobile phone companies can trace calls and ensure that any further calls and texts from that number are blocked
- internet service providers can trace messages being sent from a personal email account and can block further emails from the sender
- where bullying takes place in chat rooms, the child should leave the chat room immediately and seek advice from parents; bullying should be reported to any chat room moderator to take action
- website providers can remove comments from social networking sites and blogs and in extreme cases, can block the bully's access to the site
- the child could change mobile phone numbers or email addresses.

Where cases of online bullying involve significant harm to the victim, advice should be taken from Camden's online safety contact officer or a MASH social worker on whether to make a referral to CSSW and/or report the incident to the police. These will be incidents where the bullying is, for example:

- extreme, for example, threats against someone's life
- involves sexual bullying or harassment
- continues over a period of time
- involves several perpetrators or may be gang related
- has a considerable impact on the victim.

5.2 Inappropriate contacts and non-contact sexual abuse

Concerns may be raised about a child being at risk of sexual abuse as a consequence of their contact with an adult they have met over the internet. Children and parents should be advised how to terminate the contact and change contact details where necessary to ensure no further contact. Parents should be advised to be vigilant of their child's internet use and report any concerns or incidents.

Children may also be sexually abused on-line through video messaging such as Skype. In these cases, perpetrators persuade the child concerned to carry out sexual acts while the perpetrator watches/records. The perpetrators may be adults but may also be peers.

In the event of an incident, the child should be taught how to use the CEOP "Report abuse" button (normally displayed on the screen) and parents should contact the police to report the incident.

Staff and parents should contact Camden's online safety officer or MASH social worker for advice on making a referral where there are concerns that the child:

- is being groomed for sexual abuse
- is planning or has arranged to meet with someone they have met online
- has already been involved in making or viewing abusive images
- has been the victim of non-contact sexual abuse.

If parents are aware that a child is about to meet an adult they have made contact with on the internet, they should contact the police on 999 immediately.

5.3 On-line child sexual exploitation (CSE)

CSE describes situations where a young person takes part in sexual activity either under duress or in return for goods, food or accommodation. A key element of CSE is that there is a power imbalance in the relationship, for example often the perpetrator is much older than the child, who may not aware that they are being abused.

Staff should be aware that children can be sexually exploited on-line, for example posting explicit images of themselves in exchange for money or goods.

If staff are concerned that a child they work with is being sexually exploited on-line, they should complete the CSE risk assessment available on the CSCB website. Where indicated by the risk assessment, staff should consider making a referral to CSSW and may discuss this with Camden's online safety contact officer or the MASH social worker.

For further details, staff should refer to the CSCB guidance on CSE available at: http://www.cscb-new.co.uk/wp-content/uploads/2015/09/Multi-Agency Guidance On Child Sexual Exploitation_2015.pdf

5.4 Contact with violent extremists

Many extremist groups such as far right groups, animal rights activists and Islamic fundamentalists 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 and may become radicalised.

Camden has a duty under the government's Prevent strategy to divert young people away from extremism. To achieve this, Camden has a Channel Panel that provides multi-agency support to young people at risk of radicalisation. Staff can refer young people they are concerned about to the Panel and can seek advice from the Channel Panel co-ordinator about making such a referral.

- Staff need to be aware of those young people who are being targeted by or exposed to harmful influences from violent extremists via the internet. Young people should be warned of the risks of becoming involved in such groups and it should be against service policy to access such sites.
- Services should ensure that adequate filtering is in place, with a review of filtering taking place whenever there is any incident of a young person accessing websites advocating violent extremism.
- The service online safety contact officer should record and review all incidents in order to establish whether there are any patterns of extremist groups targeting the service and an online safety incident report should be sent to Camden's online safety contact officer and the Channel Panel co-ordinator.
- If there is evidence that a young person is in contact with extremists and being radicalised, staff should seek advice from the Channel Panel co-ordinator and consider making a referral to the Panel.

 A referral should be made to CSSW where the child is deeply enmeshed in the extremist narrative and there is evidence that their parents are involved in advocating extremist violence or there are fears that a younger child may be at risk due to their parent's extremism and may be brought to a conflict zone.

For further details, staff should refer to the CSCB guidance on safeguarding children and young people from radicalisation and extremism available at: http://www.cscb-new.co.uk/wp-content/uploads/2016/03/CSCB-guidance-on-radicalisation-and-extremism.pdf

5.5 Websites advocating extreme or dangerous behaviours

Some internet and social media 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.

Services should provide young people with an opportunity to discuss issues such as self-harming and suicide in an open manner and support any young person who is affected by these issues.

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.

Where staff are aware that a young person is accessing such websites and that this is putting them at risk of harm, they should consider making a referral to CSSW.

5.6 Sexting and sexual abuse and harassment by peers

The internet contains a high level of sexually explicit content and internetbased 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" is the sending of sexual images between young people via the internet or mobile devices and producing and sharing these images is illegal. Young people 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. Distributing images may also be a criminal offence under the Sexual Offences Act 2003.

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:

NCA_Sexting_in_Schools_WEB_1_.PDF

Staff need to be aware of the use of IT for the purpose of distributing unsuitable materials and sexually harassing other young people and be able to safeguard young people from this. Where there are concerns about a young person's online behaviour involves sexually harmful behaviour towards another young person, staff should refer to the CSCB *Harmful sexual behaviour protocol* available at: link

Staff should also be aware of when any of these behaviours may be linked to the sexual exploitation of a young person 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

6 Responding to child protection incidents

6.1 Role of CSSW

As the statutory agency for child protection, CSSW has the key responsibility for investigating online safety incidents where the child is thought to be at risk of suffering significant harm. Incidents where an online safety incident raises child protection concerns will be investigated via child protection procedures.

CSSW will also investigate online safety incidents that involve inappropriate internet use by members of the children's workforce where this raises concerns about the person's continued fitness to work with children.

These cases must be referred to the Local Authority Designated Officer (LADO) based in the Children's Quality Assurance Unit of CSSW and will be dealt with under the Camden Safeguarding Children Board policy *Managing allegations against staff* available at; http://www.cscb-

new.co.uk/downloads/LADO/Managing%20allegations%20against%20staff%20and%20volunteers%20-%20multi-agency%20guidance%202011.pdf

6.2 Referral to CSSW

Whenever a professional is concerned that a young person they work with is at risk of harm due to their internet use, they should discuss their concerns with the online safety contact officer for their service and seek advice from Camden's online safety contact officer and/or the MASH social worker regarding whether to make a referral. For cases involving radicalisation and extremism, the Channel Panel co-ordinator may also be approached for advice.

All referrals should be made to the MASH team using an e-CAF referral form. An online safety incident record should also be completed and sent to Camden's online safety contact officer. Where there are concerns about child sexual exploitation, a CSE risk assessment should be completed and sent with the referral.

Referrals should be made where there is evidence of any of the following:

- The child is in contact with unsuitable adults and is either being groomed for or already involved in on-line sexual abuse, for example via web-cam.
- The child is either being groomed for or involved in on-line child sexual exploitation.
- The child is either the victim or perpetrator of extreme online bullying, including bullying or harassment that is sexual or racist in nature; in these cases a referral should be made for both children as CSSW will need to consider the needs of both children.
- The child is in contact with violent extremists and has become enmeshed in the extremist narrative, and their parents may support these views.
- The child persistently accesses and distributes violent, pornographic or otherwise inappropriate materials.
- The child is accessing websites advocating suicide, self-harm or other dangerous behaviours and there are concerns about their emotional wellbeing.
- An adult member of the child's household is accessing or distributing child sexual abuse images.

6.3 Action by CSSW

All online safety incidents involving risk of significant harm should be dealt with via the child protection system and a strategy discussion initiated in line with the London Safeguarding Children Board child protection procedures.

Part A: Core Procedures - London Safeguarding Children Board: Child Protection Procedures

Issues that will determine whether there is a risk of significant harm will include;

- the extent of harm and the level of perceived risk to the child and other children
- involvement of adults who pose a risk to children
- whether parents are able to adequately protect their child from harm and take the risks posed seriously.

Social workers should be aware that issues around online safety may arise during assessment of other presenting issues, for example a child who exhibits sexually harmful behaviour may be accessing adult websites, or a vulnerable child may be placing themselves at more risk through their contacts on social networking sites.

Strategy discussions should consider the following:

- all available electronic evidence of grooming, abuse, harassment or bullying or the distribution of inappropriate images of the child
- the involvement of any adults who pose a risk to children, whether they can be identified and what action can be taken against them
- whether other children are involved in any abuse, either as victim or perpetrator
- the needs of all children involved, including perpetrators
- whether the matter should be investigated under the organised and complex abuse procedures where there is more than one victim or perpetrator
- the nature of the risk to the child and evidence of harm
- the ability of parents to take action to protect their child.

The Police CAIT should be involved in any strategy discussion and subsequent investigation and where the names of any involved adults are known, the CAIT should carry out checks and gather any relevant information and may contact the Child Exploitation and On-line Protection Centre (CEOP) to help trace perpetrators on-line.

6.4 Children known to CSSW

If during the course of working with a child social workers become aware of a serious online safety incident that has happened at home and which raises child protection concerns, the social worker should complete an online safety incident report. The report should be sent to Camden's online safety contact officer and shared with a child protection IRO to get advice on what action to take.

Social workers need to work closely with parents and carers to ensure children are safe when using the internet, especially if there are concerns about the child's use or they are particularly vulnerable.

In particular, social workers may wish to discuss the level of supervision a child may need to keep them safe on-line and what practical actions parents can take to improve internet safety, such as use of filters and parental controls. Information for parents on online safety can be found in the division's online safety policy and resource folder.

Parents and carers need to know about the risks posed by ICT so that they are able to continue online safety education at home and regulate and supervise children's use as appropriate to their age and understanding. Social workers should ensure that they have a copy of Camden's internet safety guide for parents available at: <a href="https://link.com/l

6.5 Parent's use of the internet

Parents own use of the internet may raise concerns, for example, around accessing pornography on the internet. Where there is evidence that an adult in the household is viewing child sex abuse images, this will require a child protection response as it raises serious questions about the safety and welfare of children living in the household and who are in contact with the adult.

In such cases, the matter will need to be dealt with jointly by the Police Child Abuse Investigation Team (CAIT) and CSSW. Social workers should refer to section 5.23 of the London child protection procedures for details on what action needs to be taken.

7 IT and safe working practice

All professionals who work directly with children 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 children.

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 children should only be taken as part of a clear work objective that has been agreed with managers and should be stored on work equipment.
- Staff should only use work equipment and only store images on their work computer, 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 children 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 and will not affect their professional standing or the integrity of their service or organisation.
- Staff should not breach confidentiality by making any comments to do with specific children via the internet.
- Staff should not engage in any conversation with children via their private instant messaging or social networking sites as these may be misinterpreted or taken out of context.
- When making contact with children or parents by telephone, staff should avoid using their own phones. Children's or parent's numbers should not be stored on a staff member's personal mobile phone and staff should avoid lending their mobile phones to children.
- Staff should ensure that personal data relating to children is stored securely and encrypted if taken out of the office.

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

All staff will be bound by their terms of employment and code of conduct and these are likely to cover confidentiality and professional standards. Further, many members of the children's workforce will also be bound by professional rules regarding their conduct. Such rules are likely to cover use of the internet and it is recommended that all staff are aware of any standards of behaviour expected from their employer or their professional body.

Appendix 1

Online safety incident report form

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

School/organisation's details:

Name of school/organisation:		
Address:		
Name of online safety co-ordinator:		
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 (online bullying) deliberately bypassing security or access hacking or virus propagation racist, sexist, homophobic, transphobic, bi-phobic religious hate material terrorist material online grooming online radicalisation child abuse images on-line gambling soft core pornographic material illegal hard core pornographic material other (please specify)		
Description of incident		

Nature of incident

D. III		
□ 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 □ online 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 LADO referral made to LADO incident reported to police incident reported to Internet Watch Foundation incident reported to IT disciplinary action to be taken online safety policy to be reviewed/amended Please detail any specific action taken (ie: removal of equipment)		
□ Child/young person		
 incident reported to head teacher/senior manager advice sought from Children's Safeguarding and Social Work referral made to Children's Safeguarding 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 online safety policy to be reviewed/amended 		
Outcome of incident/investigation		