**SAFEGUARDING AND SUPPORT**

**E SAFETY GUIDE AND POLICY**

**INTRODUCTION**

1. This document does not supersede any agreements included in the Council’s terms and conditions of employment or expectations included in the corporate acceptable use policy or social media policy. All employees should ensure they are aware of the requirements of these policies which are available on the intranet.
2. While acknowledging the benefits of internet usage it is also important to recognise that there is a risk to children and young people from this type of technology. It is known that some adults may use the internet to pose as someone from a peer age group and attempt to befriend or meet up with children and young people. In addition to this there is information on the internet concerning weapons, crime, racism, drugs etc., that it is considered inappropriate to access.
3. E safety is about keeping children and young people safe from the risks to personal safety and wellbeing when using devices that allow access to the internet as well as those that are used to communicate electronically. This includes mobile phones, gaming consoles, social networking etc.
4. In order to ensure that children and young people are safe on line and are informed of the potential dangers, employees need to have an awareness of the types of sites that children and young people use and the risks associated with them.
5. All employees are expected to attend the training available. This can be accessed via the training section.
6. This policy document aims to provide employees with:
* an awareness of the dangers and risks faced by children and young people using electronic technology;
* guidance for dealing with e safety issues and consequences for children young people, particularly those in care;
* an appreciation of professional boundaries and electronic technology
* a reminder of the Council’s expectations on internet usage by employees and the code of conduct.
1. Foster carers should be referred to the foster carers handbook for advice on E safety. The CEOP information sheet will be made available for adopters.

**WORKING WITH CHILDREN**

**Risks**

**Internet usage (including computers, laptops and mobile devices)**

1. Looked after children should have age appropriate filters and security settings on equipment that they have access to. Social workers and foster carers should discuss the reasons for this with them.

 **Web cams**

1. Young people should be cautioned to ensure that web cams are properly turned off or covered securely when they are not in use. There is a risk that unless this is done it may be possible for someone to hack into the computer and watch the young person without them being aware of this.

**Mobile phones**

1. The majority of mobile phones have internet access capability and many young people use their phones in a similar way to a computer. It is therefore possible for young people to have instant and unsupervised access to the internet via their mobile phone. Virtually all phones have cameras and videos. This has led to the rise of incidents of violence and/or abuse being recorded and broadcast and “sexting” where users record and send indecent images or explicit text messages. Images and messages broadcast in this way are beyond the owner’s control once they have been sent.

**Inappropriate contact – parents/family members and looked after children**

1. There is a risk that parents and family members who are not permitted to make contact with children in care, or whose contact is restricted, may use social networking and twitter etc. to make direct contact with children in care.

**Grooming**

1. Adults who wish to abuse children or young people may pose on the internet as a peer to attempt to make contact and/or meet up with them. The process of grooming may take place over a period of many months using chat rooms, social networking, gaming etc.

**Instant messaging & photo/video sharing**

1. Instant messaging is a form of simultaneous real time text communication over the internet. Unlike chat rooms where users are able to speak to strangers in a shared space, instant messaging takes place between people who possess each other’s contact details. There is a risk that young people may compromise themselves by sending images and/or inappropriate information. Once these have been shared the child young person has no further control over them. Unlike some chat rooms instant messaging is not moderated.
2. Instant messaging applications such as “snap chat” and “instagram” can be used to share photos and videos on line. Young people may not realise that if a screen shot is taken of the message or picture sent, it may be retained and distributed by the recipient in a way that the young person had not intended. Images and messages broadcast in this way are beyond the owner’s control once a screen shot has been taken

**Chat Rooms**

1. The ability to converse with multiple people in the same conversation differentiates chat rooms from instant messaging, which are more typically used for one-to-one communication. Chat rooms may be set up to connect people with shared interests and sometimes have rules that users are expected to follow particularly in rooms designed for children.
2. Some chat rooms are moderated either by limiting who is allowed to “speak”, by having comments approved by moderators (often presented as asking questions of a guest or celebrity), or by having moderation volunteers patrol the venue watching for undesirable behaviour. There is a risk that children and young people may form “friendships” with adults posing as peers with similar interests or other undesirable persons.

**Social networking**

1. Social networking includes sites such as Facebook, Bebo, and My Space, and sites aimed at younger children such as Moshi Monsters and Club Penguin. They allow users to build up networks of friends and mutual friends. They can be used to keep in touch, express opinions, play games, share information, videos, music and photos. Many of the risks associated with chat rooms are applicable to social networking sites with the addition that they are not moderated. Age restrictions applied by most sites can be easily overridden by most young people and are often not compulsory. There is a risk that children and young people may form “friendships” with adults posing as peers with similar interests or other undesirable persons. There is also the risk that they may be subjected to/observe or hear inappropriate language and conversations. There is also a link with cyber bullying (see separate paragraph). Providers usually provide an alert button to be used if users feel that a post is inappropriate or they feel uncomfortable with a particular participant.

**Gaming**

1. On line gaming provides young people with the opportunity to play games over the internet and to interact with other gamers within their own friendship group or across the world. This can involve web based games (i.e. World of Warcraft & Envoy) or via games consoles (i.e. XBOX, PlayStation and Nintendo). On line gaming involves real time where players can interact and speak with each other to complete missions or tasks in pursuit of virtual rewards. As above, there is a risk that children and young people may form “friendships” with adults posing as peers with similar interests or other undesirable persons. There is also the risk that they may be subjected to/observe or hear inappropriate language and conversations. There is also a link with cyber bullying (see below). Gaming platforms are not usually moderated but there is often the facility to report abusive and inappropriate behaviour.

**Cyber bullying**

1. Cyber bullying is bulling through the use of information technology and can include sending threatening or abusive e mails or texts, making insulting comments, or making and sharing derogatory or embarrassing videos. Once information has been shared it is out of the originators control and the abuse can spread causing more distress to the victim.

**Supporting victims and managing incidents**

1. Where there has been inappropriate contact between a looked after child and a parent or family member, the child must be given practical support to terminate communications and arrangements should be made to ensure that the contact does not resume. Contact must be made with the parent or family member responsible who should be advised of the consequences of repeating the unauthorised contact.
2. Where a looked after child or young person has been the victim of bullying, abuse or inappropriate behaviour on line the worker should identify appropriate support in line with the child protection policy. A note should be made on the child’s record and the carer informed. The child should be advised not to respond to the abusive contact. Evidence (text messages/emails, etc.) should be saved and the Police contacted as appropriate. Police should always be contacted in instances concerning illegal activity, grooming etc. Contact should be made with on line providers to have posts/images removed. If the perpetrator of abusive communication is a looked after child the carer or allocated worker should discuss the consequences with them with a view to education and consider any age appropriate sanctions if deemed necessary.
3. Where a looked after child has viewed what is considered an age inappropriate website the carer or allocated worker should discuss this with them with the aim of providing guidance, education and age appropriate support. Checks should be made to ensure that filtering and security settings are age appropriate.
4. If a looked after child has used the internet inappropriately the consequences should be discussed with them by the carer or allocated worker with the aim of educating them of the risks and dangers involved. Activity that might be illegal should be discussed with the Operations Manager.
5. The following advice may be helpful for employees when considering what information to give children and young people:
* Ask permission before using the internet
* Tell your carer or a trusted adult if you see anything that makes you feel uncomfortable
* Immediately close any webpage you feel uncomfortable with and report to a trusted adult or use the online CEOP button.
* Do not give out any personal information such as name, address, telephone number, age, school, bank details
* Do not give out any passwords and use strong passwords (i.e. not something that another person could easily guess)
* Ensure you set the correct privacy settings on social networking websites so that not everyone can see your details, pages and photos
* Only contact people you have actually met off line
* Only accept friend requests from people you have actually met off line
* Never arrange to meet someone you have only met on the internet
* Only use a webcam with people you have met off line and know
* Think very carefully about any pictures and comments you post on line as these may be forwarded on without your knowledge or permission and become out of your control.
* Never be abusive or unkind to anyone on the internet
* Only open e mails from people/ organisations you recognise
* Avoid using website that you are not happy to tell anyone about
* Use a student friendly search engine (i.e. <http://www.askforkids.com>)

**EMPLOYEE ISSUES & PROFESSIONAL BOUNDARIES**

**Internet usage (including computers, laptops and mobile devices)**

1. Whilst at work or using Council equipment employees must not visit internet sites, make, post, download, upload or pass on material remarks, proposals or comments that contain or relate to:
* Indecent images of children
* Promoting discrimination of any kind
* Promoting racial or religious hatred
* Promoting illegal acts
* Violence and bomb making
* Illegal taking or promotion of drugs
* Adult pornography
* Other information that may be offensive to others
1. Illegal activity will be reported to the Police. Employees should refer to the Council’s code of conduct (<http://inside.ealing.gov.uk/downloads/download/18/code_of_conduct>). Acceptable use policy (<http://inside> ealing.gov.uk/download/downloads/id/605/acceptable\_use\_policy), and social media policy (due on the intranet early in 2014). Social workers should also refer to the HPC “standards of conduct performance and ethics”

http://www.hpc-uk.org/aboutregistration/standards/standardsofconductperformanceandethics/)

1. Employees need to be aware of professional boundaries and expectations in relation to the internet and electronic technology usage. Employees should not take photos or videos of children using their personal equipment. Employees should use a Council owned and approved device for permitted photography. Employees must ensure that photos and videos are stored appropriately and that once photos or videos have been uploaded or printed as required they should be deleted from the original device. Employees must ensure that any images temporarily taken home (i.e. if on a trip or visit and the worker cannot return equipment to the office until the next working day) images must be stored securely and in line with data security expectations.
2. Employees must consider and review the way they use social networking. Security settings should be used to control access to profiles. Employees need to be aware that once published, information including photographs and posts, may be manipulated without consent, used in a different context or distributed in an uncontrolled way.
3. It is not appropriate for employees to have clients as friends on their social networking site. It is also important for employees to avoid detailed discussion about work on social networking sites to avoid any unintentional lapse in confidentiality. Employees should not upload any work related images (for example photos/videos taken on trips) or “tag” their location. Employees should only use Council provided equipment to make electronic contact with children and young people. In addition employees should ensure that all electronic contact with clients is noted in FWi.
4. If in doubt employees should contact their Manager for advice and/or refer to the Code of Conduct (see para 21)
5. Foster Carers should exercise caution when using social networking sites not to inadvertently reveal details of children they are looking after. Detailed guidance for carers can be found in the handbook.

**Reporting abuse and misuse**

1. It is the responsibility of all employees and foster carers to report any abuse and misuse of the internet by colleagues to their line manager in the first instance. Employees should refer to the councils Whistleblowing Policy.

 <http://inside.ealing.gov.uk/downloads/download/224/whistleblowing_policy>

1. Employees should also notify the LADO named officer for allegations against employees (currently Ruth Lacey) within 1 working day, and ensure compliance with CP procedures <http://www.londoncp.co.uk/procedures/15_alleg.html>.
2. Where there has been inappropriate or illegal use of the internet by an employee:
* Employees may be subject to the Council’s disciplinary process. Accessing certain sites may be considered gross misconduct and may lead to dismissal without notice.
* Serious breaches and illegal activity will be reported to the Police. The relevant Operations Manager and/or LADO must be contacted before this is progressed. A decision will be made as to whether to refer the incident to the audit and investigation team.
1. If concerns are raised about an employee or representative of another agency these should be reported immediately to the Operations Manager and/or LADO.
2. Where an employee is suspected of accessing illegal or inappropriate sites or has been accused of inappropriate conduct via electronic media the employee Code of Conduct and Council disciplinary procedures apply. An immediate referral should be made to the Operations Manager who will contact the LADO and HR to instigate an investigation under the Councils agreed procedures. An early decision needs to be made as to whether the incident should be reported to the Police and/or the Council’s Internal Audit and Investigation Team and the allegations against professionals process should be instigated as appropriate.
3. Depending on the circumstances, and if the allegations against professionals procedure has been implemented, a decision may be made to suspend an employee while the investigation is on-going. HR will provide support and advice during the implementation of the relevant protocols. Actions might include escorting the employee to his/her work station to retrieve **personal effects only**. Employees may be instructed to hand over all keys and access cards and all Council equipment including mobile phones, computer tablets, cameras etc. Arrangements should be made to have the employees access to Council systems suspended pending the result of the investigation. It may be considered appropriate to advise the employee not to contact any members of staff or clients direct.