INTERNET AND TELECOMMUNICATIONS POLICY

J&R Care Ltd believes that the use of information and communication technologies in its homes and schools bring great benefits. Recognising the esafety issues and planning accordingly helps to ensure appropriate, effective and safe use of electronic communications. The internet is an essential element for children and adults in the 21st Century life for education, business and social interaction. J&R Care have a duty to provide residents and pupils with quality internet access as part of their learning and development.

Children will use the internet widely when outside of the home and at school and will need to learn how to evaluate internet information and to take care of their own safety and security.

J&R Care Ltd recognise the risks in allowing children and staff to use the internet:

Communicating online can be a fantastic experience for children.

They can use a number of different applications including Chat Rooms, Instant Messenger, Blogs, forums and gaming sites. Chatting online is often an innovative way to share homework tips, learn new social skills, and build new relationships.

Although chatting online can be great fun, children can sometimes find themselves in situations where they can feel out of their depth. Risks can arise when children give out their personal details to strangers. The online world can often seem very different to the real world for children, and they can be tempted to say and do things that they wouldn't dream of if they met someone face to face.This can include giving out personal information such as mobile numbers and pictures of themselves. If they are talking to another child there is a risk that they will misuse this information - for example, by texting abusive messages to the child, or by posting their image on a website; but there is obviously a greater risk if the person that they are chatting to is an adult. Unfortunately, paedophiles - adults who want to meet children for sex - use the internet, often with the intention of talking with and meeting a child. Children can be naive to this risk, and often feel that they are invincible, or that 'they would know if someone was lying'.

Children will often 'swap friends' through IM, and therefore can be chatting to strangers who they feel they trust because a friend of a friend knows them. IM is a very intimate form of communication - more so than a chat room with many participants, and therefore child abusers will often use this as a means to extract personal information from a child.

Child sex abusers find the internet an easier place to participate in a range of child sexual abuse activity including contact with children due to the anonymity of the medium. They will often lie and pretend to be younger than they are or people other than themselves, and find a sense of security by operating from the safety of their own homes. They have been known to set up bogus email accounts and chat personas to mask their identity online.

There are a number of actions which these adults will engage in online. These include:

- Swapping child abuse images in chat areas or through instant messenger with other adults or children and forming networks with other child abusers to share tips on how to groom more effectively and how to avoid being caught.

- Swapping personal information of children that they have collected with other abusers

- Participating in online communities such as blogs, forums and chat rooms with the intention to groom children, collect sexually explicit images and meet them to have sex.

- Online Grooming is:

"A course of conduct enacted by a suspected paedophile, which would give a reasonable person cause for concern that any meeting with a child arising from the conduct would be for unlawful purposes."

Often, adults who want to engage children in sexual acts, or talk to them for sexual gratification will seek out children who desire friendship. They will often use a number of grooming techniques including building trust with the child through lying, creating different personas and then attempting to engage the child in more intimate forms of communication including compromising a child with the use of images and webcams. Child sex abusers will often use blackmail and guilt as methods of securing a meeting with the child.

Gaming

Gaming can be great fun, and can be a place where children play and chat - mostly about the game - to each other. Gaming sites can be fantastic fun for children, however as with any online technology - there are risks.

Online gaming can occasionally be addictive for children. They can become so involved in the gaming communities that they lose touch with their offline friends, in favour of spending time with online users playing games. Some children who use online games can be abusive to other gamers. This can range from saying nasty things if there is a chat facility within the

gaming site, to always winning and not sharing cheats or knowledge on how to progress to the next level. Children should be encouraged that when they play online games, they treat others how they would like to be treated.

There are some children who engage in risky behaviour to obtain cheats or knowledge to progress within a game.

Is is because of the above risks that it is necessary to put into place a statement and policy guidelines on the use of the internet for children in our homes.

J&R Care Ltd are committed to ensuring children's safety online and have developed a policy on its use in the home and school:

Our internet safety policy has been written by the directors of the company, building on the Kent County Council's e safety policy and guidance.

J&R Care Ltd has an Internet Safety Officer who will ensure that:

- The homes/schools internet access is designed expressively for residents/pupils use and will include filtering appropriate to the children's age and understanding.

- Residents will be taught what internet use is acceptable and what is not and given clear objectives for its use.

- The computers in the home/school have been positioned in all areas to allow easy supervision of the work/content being displayed and hence discourages breaches of acceptable use.

- Staff will guide the child in online activities that will support the learning and development planned for the child's age and maturity.

- No child will have access to the internet without consultation with a member of staff and the access will be supervised and monitored.

- The company and its staff will ensure that the copying and subsequent use of the internet complies with copyright law.

- The security of the homes/schools computer will be inspected and updated every six months.

- Virus protection will be updated regularly.

- Portable media may not be used without specific permission by the Internet Safety Officer who will instigate a security check on the system.

- Files, web sites and emails on the homes/schools network will be regularly checked and monitored.

- Children and Staff may only use approved email accounts.

- A central email address for staff and one for each child will be set up and the only email addresses used.

- Access in the home/school to personal email accounts is prohibited by both staff and children. Email sent to external organizations should be written carefully and authorized by a senior member of staff before sending.

- The forwarding of chain letters is not permitted.

- No resident /pupil or staff member will be authorized to place photos on any social network space.

- The use of web cams in the home/school is strictly prohibited, unless for specific supervised pieces of work within the school.

- Emerging technologies will be examined for educational/social development benefit and a risk assessment will be carried out before use in the home/ school.

- The home school will maintain a current record of all staff and residents activity online and will be signed by the manager of the home and stored in the main office.

- Social workers/parents will be asked to sign a consent form for resident's access in the home.

- An e safety training programme will be introduced to raise awareness of the importance of safe and responsible internet use.

- Staff and children will be asked to sign an internet code of conduct before being allowed to use the internet.

- The use of the computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990

- Complaints of internet misuse will be dealt with by the Internet Safety Officer and the Directors and discussions will be held with the local police to establish procedures for handling potential illegal issues.

- Consequences within the home for misuse of the computers/internet will include: Investigation by the ISO/directors; informing social workers/parents; removal of the internet or computer access for a period of time.

- Staff who misuse the computer/internet will be dealt with through the companies disciplinary procedure

- Any staff member found to be interfering or deleting any monitoring system will be dealt with through the companies' disciplinary procedure.

All staff will familiarize themselves with legal documentation relevant to internet safety, use and abuse, which include:

- The Sexual Offences Act 2003 , which introduces new offences of grooming and in relation to making/distributing indecent images of children, raised the age of the child to 18 years old.

- The Racial and Religious Hatred Act 2006 which creates new offences involving stirring up hatred against persons on religious grounds.

- The Police and Justice Act which extended the reach of the computer misuse Act 1990 making denial of service attacks a criminal offence.

- Communications Act 2003 (Section 127)

- Data Protection Act 1998 (Sections 1-3)

- Malicious Communications Act 1988 (Section 1)

- Copyright, Design and Patients Act 1988

- Public Order Act 1986 (Sections 17-29)

- Protection of Children Act 1978 (Section 1)

- Obscene Publications Act 1959 and 1964

- Protection from Harassment Act 1997

- Regulation of Investigatory Powers Act 2000

- The Telecommunications (lawful business practice)(Interception of Communications) Regulations 2000

Mobile phones

Whilst J&R Care Ltd will tolerate staff using mobile phones for essential calls during working hours i.e. if on an outing and a work mobile is not available, excessive use for personal calls is prohibited.

Also prohibited are lengthy calls, casual chats, text messaging, e-mailing web, browsing and the taking of video and/or still images (if your phone is so enabled). Your mobile phone should be set to a silent ring during working hours. If you wish to use your mobile phone, you are requested to do so by first seeking permission from a Manager.

No pupil should bring a mobile phone to school. If a mobile phone is brought into the classroom, the teacher will ask that it is handed over to them. If the child refuses, they will be asked to leave the room.

Updated February 2013