E-Safety Policy

The internet has become an integral part of our lives. A world has been opened up which offers many positive opportunities. The use of information and communication technologies (ICT) is of great benefit to children/young people and provides a new world for them. It offers entertainment opportunities for education, information and communication. It is clear that children/young people get a lot of benefit from being online and looked after children/young people should have the same opportunities as other children/young people.

Children start using computers from a very early age and are increasingly using the internet more and more whether it is at home, in school, on their mobile phones or on a games console. With this in mind, internet safety and knowing how to help protect children/young people online is essential.

Just as we want to keep children/young people safe in the real world, we will want to do the same in the virtual world. It is important that we understand enough about the internet to keep them safe from harm but is equally important that we equip our children with the skills they need to keep themselves safe so they can experience the internet positively and responsibly.

The 'online' world, like the rest of society, is made up of a wide array of people and experiences. Whilst most of them are decent and respectful, we have to remember that there are also "bad" people whose sole objective is to target the vulnerable and unsuspecting and whose interests are in abuse, corruption or other illegal activities. These are the people and sites on the internet that we wish to protect children/young people from and these guidelines are intended to support and help in this task.

We should be aware that internet access can be gained from a variety of mediums such as computers, mobile phones, computer games, tablets e.t.c. Free wi-fi access is available to all children/young people in various locations and as such we need to be clear that despite staff vigilance, children/young people will have access to the internet outside of the home and as such we need to ensure we make children/young people aware of possible dangers of social networking, online grooming and on line gaming,

Children/young people accessing the internet are vulnerable and may expose themselves to danger, whether knowingly or unknowingly. Children/young people may be exposed to cyber bullying, sexting, inappropriate material, in particular criminal activity by paedophiles, and child pornographers and additionally, there is information on weapons, crime, drugs and racism, access to which for children/young people would elsewhere be restricted. An innocent search may take them to a site exposing them to adult content or violent imagery.

Most internet use is safe, purposeful and beneficial to children/young people. It can increase their feeling of independence and supports their learning. Recognising e-safety issues and planning accordingly helps ensure appropriate, effective and safe use of electronic communications.

The Together Trust will endeavour at all times to protect children/young people who use the internet, highlight potential dangers and raise awareness about safe use of the internet.

The Together Trust believes that when children/young people are supported to access the internet in a safe and positive manner this enhances their life chances and knowledge.

Associated Policies:

- Safeguarding Children/Young People Policy and Procedure (Service)
- Safeguarding Children/Young People Detailed Guidance (Service)
- Counter-Bullying and Bullying Policy and Procedure (Service)
- Mobile Telephone/Handheld Device/Social Media and website use at work Policy and Procedure (Service)

E-Safety Procedure

1. RULES AND GUIDELINES

(a) Children/young people need to understand the rules given to them must be followed. They need to learn e-safety rules in a way that does not frighten them and which gives them confidence to know what to do in certain situations. They need to understand the rules will change and develop as they get older. They need to learn how to apply strategies which will help them avoid certain 'risks'.

(b) All children/young people are made aware on admission to Together Trust services of the systems that are in place for the safe monitoring of I.T., email and internet usage. All computer systems available to the children/young people in the homes are maintained by the Together Trust's I.T. department and are protected by appropriate anti-virus software and parental controls. The use of chat rooms and any other similar websites must be screened for use by the home's manager; the I.T. department must be consulted if in any doubt.

(c) It is the Together Trust's policy to ensure that all children/young people accessing the internet from a home's computer should be supervised in line with their risk assessment in a supportive manner.

(d) Staff must ensure that if the home has a wireless network, the key for internet access must not be disclosed to the children/young people. Children/young people should not be given wireless access to the internet on their personal computers/laptops or mobile devices.

(e) Staff should monitor the behaviour of children/young people when they access the internet, and intervene if they believe a child/young person may be at risk.

(f) All computers with internet access should be installed in communal areas within the home but not allowed to dominate.

(g) Careful consideration/risk assessment by both staff, the child/young person's Social Worker and parents if appropriate, should be given to children/young people who request a computer in their bedrooms.

(h) Staff must not allow children/young people to use any computers in the office.

(i) Staff should not use a computer that is for the use of children/young people for the writing of material regarding any aspect of work.

(j) Staff should be aware of the risks to children/young people through the use of social networking sites on the internet.

(k) Children/young people should be aware that once they have sent an image or posted it online, they no longer have control of it, they cannot get it back and that it could end up anywhere. Ask them how they would feel if their parents, teachers or their whole school saw what they had sent.

(l) Children/young people need to be aware that publishing personal information could compromise their security and that of others. Social networking sites such as Bebo, My Space, Facebook, Twitter and Piczo allow children/young people to set up an account and create a web page containing personal information e.g. age, name, email address, phone number, school, likes, dislikes, photos, videos in minutes. Information given by users is not checked and there are very limited safeguards. Offenders and paedophiles target and groom children/young people, gaining their trust and confidence, in preparation to progressing to other forms of contact, such as text messaging, as a

prelude to meeting in person or committing online abuse. These techniques are often known as 'online enticement', 'grooming' or 'child procurement'.

(m) Online bullying is also an unfortunate feature of increased access to technology. It is perceived as providing an anonymous method by which bullies can torment their victims at any time of day or night. Whilst a child/young person may not be in physical danger, they may receive e-mail, chat or text messages that make them feel embarrassed, upset, depressed or afraid. This can damage their self-esteem and pose a threat to their psychological wellbeing. All staff need to be aware of the potential for this, and if they become concerned that a child/young person is becoming involved, as a victim or a perpetrator, the child/young person's Social Worker should be informed immediately. 'Bullying Online' is an online help and advice service combating all forms of bullying. The 'Staying Safe in Cyberspace' section gives tips for staying safe in chat rooms. There is also a section on mobile phone bullying, giving tips on how to protect yourself and information on how the law can help. You can find this at http://www.bullying.co.uk.

(n) Children/young people should not upload photos and videos of themselves or other children/young people and they should not publish personal information, such as location and contact details. Explain and be clear with the child/young person that they should **NOT** give personal details e.g. name, address, telephone number or name of school to anyone on the internet or to arrange to meet secretly any contact made through the internet or through social networking sites and they must never share their password to any one on the internet.

2. PARENTAL CONTROLS

The Together Trust ensures that on all homes' computers there are security systems/parental controls in place to restrict access to unwanted internet sites, chat rooms e.t.c. and full use should be made of these systems, whilst recognising that these systems are not "fool proof" and that no system of automatic controls is secure and risk free nor take the place of effective staff supervision.

2.1. If you are the registered administrator for setting parental controls, **PROTECT YOUR PASSWORD**. It is through you that all levels are set and your password is the key. Memorise it and do not give it to any child/young person.

2.2. The setting of 'Parental Controls' can be achieved through an Internet Service Provider supplied router/software or third party independent programs. Whichever method is in use, the process of setting the controls should be easily understood by the authorised administrator (Registered Manager).

2.3. Children/young people should not be allowed to set their own levels of access as all changes to 'Parental Controls' can only be made by the named administrator who is not going to divulge the password.

2.4. The Administrator should change their password every month and review all levels of access. They should also use a secure password containing numbers and letters and conduct occasional tests of the filter to ensure it is still functioning correctly.

2.5. After you have set parental controls, be sure to sign off and completely exit the software before allowing children/young people to sign on.

2.6. If you stay connected through your Administrator logon, anyone can edit the controls on other listed screen names. Exiting and restarting the computer will ensure that the parental controls have been fully implemented.

Just as you would discuss with children/young people what they did in school, you should talk to them about online experiences. The more involved you are with their online activities, the easier it will be to set limits that are age appropriate. The people who know best about what the children/young people are up to online, are the children/young people themselves. Get

children/young people to tell you about the sites they're using. Ask them questions and talk to them about such things as:

- Why do they like the site?
- What can they do on it?
- What's so fun about it?
- Who uses it at school?
- Who you can talk to?
- Are their friends on it?
- Ask to see their profile
- Who are they playing with? Are they friends from school or an online friend? Do they understand the difference?
- What information they should not give on line like personal information such as their name, address, telephone number or which school they go to.
- Come up with a list together of things they can share about themselves online (favourite games, films or bands; hobbies) and things which they shouldn't share (real name, address, age or school)
- Get them to show you the things they enjoy online. Ask them if they can block people who are horrible and get them to show you how – blocking is a vital digital skill

This is a good way to develop trusting relationships with children/young people about what they are doing online.

If a child/young person or member of staff suspects that the computer has been used for, or displays any of the following, the computer is to be unplugged from the wall and the I.T. department informed immediately. Do not shutdown the computer before unplugging and in no circumstances look for information on the hard drive or internet browser yourself, this may result in vital information being lost in the event of an investigation:

(a) Viruses / Malware
(b) Indecent images being displayed either accidentally or on purpose
(c) illegal software installed
(d) illegal downloading of files (music, movies e.t.c.)
(e) cyber bullying
(f) chat room grooming.

If in any doubt whatsoever, unplug the computer and contact the I.T. department immediately.

3. MOBILE DEVICES

Increasingly the internet can be accessed by a wide variety of other devices such as mobile phones, games consoles, cameras and tablets. It can be almost impossible for staff to be able to monitor the use of mobile devices or even to know when children/young people are using them to access the internet. This makes it especially important for staff to ensure that children/young people have as much information as possible to help them to keep safe whilst on line. Staff need to be talking to children/young people about the risks and should actively engage with them either individually or in children/young peoples' meetings. As mentioned below there is plenty of information available online to look at. Staff need to keep abreast of developments with the internet as it is changing all the time.

4. ADVICE AND SUPPORT TO CHILDREN/YOUNG PEOPLE USING THE INTERNET

Children/young people need to know that the following are not acceptable:

1. Sending or displaying offensive messages, pictures or videos
2. Using obscene language
3. Harassing, insulting or cyber/bullying others
4. Creating and posting offensive or illegal content on their own or other people's web pages

Children/young people need clear advice and support on using the internet, chatrooms, blogs and social networking sites.

They need to know that they shouldn't:

- Give out personal details online
- Arrange to meet strangers that they have met online
- Do anything that makes them feel uncomfortable or that they believe is not right
- Open any spam or junk mail or texts. Don't believe the content or reply to them
- Open files from people they don't know as they may contain a virus, an inappropriate image or film.

An excellent site that gives advice to children/young people is www.thinkuknow.co.uk which also provides a way for children/young people to report concerns about someone they have contact with.

The Child Exploitation and Online Protection Centre (CEOP) has been set up by the Home Office to 'safeguard children/young people's online experiences and relentlessly track down and prosecute offenders'. It also provides advice to carers and professionals at www.ceop.gov.uk.

All mobile phone sites, social media and gaming consoles have the facility to report abuse or inappropriate content/postings e.t.c.