WARRINGTON
Borough Council

E-safety policy

December

2019

Author Julia Nelson

Reviewed: September 2020

Warrington Residential Services E-safety policy

1.0 Introduction

1.1. Warrington Residential Services welcome the development of new technologies for communicating and will use them wherever they are appropriate to enhance our work with children.

1.2. We recognise it is our responsibility to take all reasonable measures to ensure that the risks of harm to children's welfare from the use of technology are minimised; and, where there are concerns about a child's welfare, we take appropriate actions to address those concerns

1.3. We also recognise the need to protect staff from inappropriate conduct from children in their personal lives and from situations that may make them vulnerable to allegations of wrongful conduct.

2.0 Definition

2.1. Our E-safety policy includes all forms of electronic communication - mobile phones, computers and other devices for email, text, instant messaging, internet access and social networking.

3.0 Compliance with our Safeguarding Policy

3.1. We will ensure that our staff follow the requirements of our safeguarding policy as well as all other relevant safeguarding legislation.

3.2. We will train our staff to follow this policy, and we will regularly monitor its implementation.

4.0 Electronic Communication

4.1. It is not appropriate to have private non-work related contact with our children using electronic communication.

4.2. We recognise that there will be times when it is necessary to use electronic communication: for example sending a text message or an email to the child, however in all instances this MUST be done using equipment provided by work, including work mobile phones and work email addresses. Staff should not give their private mobile phone number or private email address to the children.

4.3. Staff must only use electronic communication for genuine reasons relating to work with a child. Genuine reasons could include responding to a question or comment from a child, contacting them to reassure them of support, confirming arrangements for a meeting or activity or to find out where they are or what time they will be home.

4.4. Staff must not send personal photographs, or personal information to children via their mobile phone or over the internet.

4.5. Where it is possible, a record of texts sent and emails sent to the child or received from them should be kept backed up electronically for reference and made available if requested.

5.0 Social networking and Facebook

5.1. Staff must take care to ensure that any personal Facebook account, twitter or other social networking site has settings applied to prevent the children from accessing their content.

5.2. Staff must not add or accept any child (or their family and friends) to their Facebook or social network account who they are currently working with or who have been known to them in a professional capacity until that child is at least 21 years of age. If staff do accept or add any young person over 21 to their social network account, that were once known in a professional capacity, then staff should be aware of how this may be viewed negatively or questioned by others**.**

5.3**.** If a child's family or friend is known to staff or their family or friends prior to the child's admission into the home then staff must report this as soon as possible to their line manager.

5.4. If a staff member is contacted by a child on a social networking site, e.g. Facebook, they should not respond by messaging that child, even to inform them that contact in this way is prohibited. Doing so will open up the staff member's profile for the child for one month. This should instead be followed up in person at the next appropriate meeting and reported to a line manager as soon as possible.

6. 0 Use of digital and video images

6.1. The development of digital imaging technologies has created significant benefits to learning, allowing staff and children instant use of images that they have recorded themselves or downloaded from the internet. However, staff and children need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

6.2. Staff should inform and educate children about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites**.**

6.3. Written permission from parents and/or social worker will be obtained before photographs of children are published on any website / social media / local press.

6.4. Staff may take digital / video images in order to provide a record for the children but staff must follow GDPR Legislation and/or seek the children’s parent or social worker’s permission before considering sharing, distributing or publication those images outside of the home.

6.5. Care should be taken when taking digital / video images that children are appropriately dressed and are not participating in activities that might bring the children or home into disrepute.

6.6. Children must not take, use, share, publish or distribute images of staff or other children residing at the home without their permission.

7.0 GDPR

7.1. Personal data will be recorded, processed, transferred and made available according to the current GDPR legislation.

7.2. It adheres to the GDPR Policy. All staff must be trained in GDPR (mandatory training).

7.3. Personal data will be recorded, processed, transferred and made available according to the current GDPR legislation. It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.

7.4. Data held must be accurate and up to date. Inaccuracies are corrected without unnecessary delay.

7.5. Support the child's Subject Access Requests to see all or a part of their personal data held by the home.

7.6. Adheres to data retention policies and routines for the deletion and disposal of data.

7.7. Reports any data breaches to Warrington BC within 72 hours of the breach, where feasible.

7.8. At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.

7.9. Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.

7.10. Transfer data using encryption and secure password protected devices. When personal data is stored on any portable computer system, memory stick or any other removable media: The data must be encrypted and password protected. The device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected) the device must offer approved virus and malware checking software. The data must be securely deleted from the device, once it has been transferred or its use is complete.

8.0 Monitoring

8.1. No filtering system can guarantee 100% protection against access to unsuitable sites. Staff at the home will therefore monitor child's internet access via random or planned checks on the child's mobile phone, tablet, and computer or game console. Staff must ensure that each child has an internet agreement in place linked to their care plan and risk assessment which clearly sets out acceptable use, what they can and cannot access, time restrictions and permission for staff to complete planned or random checks on their internet devices.

Please see appendix at the end of this policy, which provides an example of a child's internet agreement.

Overview of online technology

Online technology has changed the way children live their lives in many positive ways. It has also brought with it safety issues that require knowledge and awareness among those responsible for their welfare. These procedures set out the arrangements for safely managing children's access to computers and use of the internet whilst in the care of the Local Authority.

Computers, game consoles, tablets, the internet and mobile phones are highly attractive to children. They are essential for keeping in touch with friends, for obtaining information and for fun. Communication technology now forms a normal part of a child's everyday life.

Residential staff have an important role to play in helping children to use communication technology in the safest way. Staff members do not require an extensive knowledge of communication technology to be able to help. Everyday parenting skills demonstrated by sharing an active interest, supervision and developing the child's ability to keep safe can be very useful.

Warrington Borough Council encourages all residential staff to support and assist children in developing skills in communication technology whilst taking sensible precautions to protect them from potential harm and exploitation in the rapidly changing field of technology.

Helping children to stay safe online will always be a major priority for Warrington Borough Council. As technology changes, new risks appear. We recognise that this can be a source of considerable anxiety to anyone who is responsible for the welfare of children. This strategy is designed to provide guidance and support to residential staff and children to ensure the most vulnerable are protected from harm.

Dangers of communication via technology

- Contact by phone or online with people who may wish to harm children
- Access to inappropriate and potentially harmful material
- Exposure to unsuitable advertising, invasion of privacy and identity theft
- Exposure to risks of cyber bulling or phone bullying
- Exposure to sexting and pressure to disseminate sexually explicit images.

Safety measures and boundaries

- Time limits on computer usage should be agreed with the child
- Appropriate internet security must be installed on the computers
- Residential staff must supervise computer use in the home to avoid children having access to inappropriate/harmful material.
- Computers linked to the internet, should be located in communal areas of the home rather than the bedroom.
- Games consoles which can access the internet must have appropriate settings installed on them. Time limits on console usage should be agreed with the child
- Any access to the internet must be linked to the child's care plan and individual risk assessment.
- Permission must be sought from the social worker, if a mobile phone with internet access is purchased for a child.

E-safety should be something that is taken into account when residential staff are assessing risks for all children. This should be evident in items such as CSE risk assessments and all staff should remain mindful when working with our children. It is the role of all staff to promote and to educate children in e-safety.

ZIP, BLOCK, FLAG IT

ZIP IT, BLOCK IT, FLAG IT

.

Warrington Residential Services supports **Zip It, Block It, Flag It** – the **Click Clever, Click Safe Code**

ZIP IT means keeping encouraging children to keep personal stuff private and to think about what they say or do online.

BLOCK IT reminds children to block people who send nasty or inappropriate messages and to not to open any links and attachments received by email or through social networks

FLAG IT is the final piece of advice. It stands for flagging up to home staff, social worker or someone in authority anything that upsets them while they are online or if someone asks them to meet up in the real world.

Teaching our children how to use the internet safely is just as important as teaching them how to cross the road using the Green Cross Code rules. So when our children are online, whether alone or with you by their side, it's also as crucial to explain to them why they should stick to the Click Clever Click Safe code.

Advice for Residential Staff

Zip it

People may not be who they say they are online so ensure children realise that adults do pretend to be children in chat rooms and on instant messaging systems. Set privacy controls to restrict access by strangers to your child's social network account.

Remember, they should not be on Facebook unless they are over 13.

Be aware that even the smallest piece of personal information placed online could be used to identify them.

Block it

Where possible we should use filters, parental controls and security settings on mobile phones and games consoles as well as on your computer and other smart technology. Remember some televisions will also need further control settings to be changed.

Warrington residential services have set preferences on the computer search engines to prevent children looking for inappropriate material, however some may have devises that are not monitored and or blocked using of certain keywords. Children therefore require advice and guidance to stay safe.

Sit with children and make sure they know how to delete emails, or remove people from instant messengers, social network sites etc.

Flag it

Encourage them to talk to a trusted adult if they encounter a problem online, or come across something they are uncomfortable with. Remind them never to meet anyone in the offline world that they have met online without you going with them.

Make them aware of the Click CEOP buttons placed on the likes of Facebook and Windows Live Messenger. This allows them to report inappropriate sexual behaviour towards them directly to the authorities.

Children's use of computers and the internet

Children's use of computers is often different from adults. Many engage in a variety of internet activities, quickly switching from one to another as their attention moves from one activity to another. These would include but are not limited to:

- Research to help with homework, projects and course work.
- Getting in touch with each other via emails, Instant Messaging (IM), chat-rooms, discussion groups or to swap files and music.
- Playing online games that can be downloaded from a website or they may play with who are online (friends or strangers).
- Listening to music; downloaded from the internet or files from friends.
- Buying online.
- Writing up project work or preparing presentations for school or College.

We need to always stay vigilant and watch for different signs and behaviours following the use of ICT and or other devises associated with social networks etc. If you believe that there are other adults and or children creating risky situations you must immediately alert the social worker, Registered Manager and any other professional deemed appropriate. If they are in immediate danger the police should be contacted.

Associated Risks of Computers and Internet Usage

The main risks of online activities are personal and technological;

Personal Risk

- **Meeting someone online**: "Luring" is the term for online behaviour that leads to these meetings and is illegal. The vast majority of reported cases relate to children over 15 years and female.
- **Loss of privacy**: Disclosing name, address, telephone number to a stranger can put the child, home, residential staff and family members in danger.

- **Getting into online fights**: Communication with text or in writing can easily escalate into emotional disputes as it is difficult to know the intensity of feelings.
- **Online bullying**: This is a common problem and the most common techniques are that children are harassed or harass others via text messaging, internet chat rooms and emails.
- **Making threats/law breaking:** This can range from being rude to committing crimes online. It can also include putting someone else in jeopardy by publishing names, addresses or phone numbers of someone they know.
- **Accessing inappropriate material**: Many websites include material that is sexual, violent or hateful, or which advocate the use of weapons or harmful substances such as alcohol, tobacco, or illegal drugs. It is possible to inadvertently come across these sites when typing an address in a web browser or when using search engines. Usually because a word is mistyped or an imprecise key word is used. Unsafe links may also appear on safe sites tempting a child to search for material that they might not otherwise come across.
- **Increased vulnerability**: It is possible for children to set up their own Web sites (at no cost). Anything posted can be seen by anyone visiting the site.
- **Misrepresented Identity:** It is easy for children to forget that when they enter a “chat room” they are in a public place and do not necessarily know the true identity of anyone in the chat room. It is also important to be aware that what may appear to be moderated chat by adults is instead software. This looks for particular words and if the words appear a moderator is notified and checks the content. If someone in the chat-room is found to be breaking the rules usually they will first be warned and then, if they persist, they can be thrown out and barred. However someone who is barred usually needs only to create a new email address. This gives them a new internet identity and they can get back in.
- **Unmonitored activity** i.e. Instant Messaging (IM): Similar to chat but unlike in some chat rooms, there is never anyone else there to monitor activity.

Technological

- **File sharing/downloads**: File-sharing and downloads creates a risk that viruses or other malignant code could be spread to the computer over the network. It is also possible for others to track online activities and send that information to third parties.
- **Computer viruses:** Or even people hacking into the computer (someone gaining unauthorised access) can cause serious damage. Some viruses can hand over control of

the computer to someone who may be far away but who can use it for their own purposes, for example send email to others. Playing online games is for example a time when the computer is particularly vulnerable to a virus.

Managing risks and promoting safe use of the Internet

Recognizing the potential threats to children on the internet is the first step to protecting them. It is important to become familiar with how the child uses the internet. It is also worth bearing in mind that some mobile phones and games consoles provide internet access.

The safe use of computers by all children with whom staff work - whether they are placed in residential care, foster care or living with their parents or other members of their family should be monitored.

The following is recommended to promote the safe use of the Internet:

- **Location**: Keep the computer with internet connection in a communal area where the child is ‘independent’ but not alone. Do not share the internet/ Wi-Fi password with the child.
- **Control**: Install filtering software and parental control software. Parental control software can be used to: control content;
- control contacts
- control shopping and privacy
- help with time management
- improve general security
- Monitor and record activity, including who the child sends emails to and blocking access to all or some chat-rooms.
- **Check**: Ask the child on a regular basis to show you the places they go to on the internet and be familiar with their patterns of use and time spent online. This will help detect any changes in behaviour that may be of concern. Watch for changes and or patterns of behaviour.
- **Monitor online relationships:** Find out whom they are sending emails to and who they are receiving them from. You should know if they visit chat-rooms or subscribe to news groups and you should understand what they do when they visit these places.
- **Review Accessibility**: It is important to have rules about the sorts of websites and materials it is acceptable for the child to access.

- **Discuss**: Talk about what they do online. Having an open relationship with the child is the key to being able to discuss with them the kinds of material, people or situations they may inadvertently or deliberately come across on the internet.
- **Be open and honest**: It is vital to openly discuss with the child the possibility of them seeing or being sent sexually explicit or other worrying material. Children may otherwise feel they may have done something wrong, and perhaps be fearful of telling you in case they get into trouble and/or have sanctions applied to them. It is precisely at this stage that children can feel most isolated and vulnerable to the control of sexual or other kinds of predators.
- **Manage and limit time**: There are no hard and fast rules about what is excessive use of the Internet as it will vary from child to child, depending on their circumstances and their online activities. Internet use for school and college should be encouraged whilst at the same time recognising that this may also need monitoring. Some children may play online games, chatting or emailing each other under the pretext of doing homework.
- **Instil caution and care**: Children need to know that unless and until they are absolutely certain of the identity of someone they are communicating with, they should proceed with caution and not necessarily accept everything a person says online at face value. **Moderated (supervised) chat-rooms**: Ask about policies enforced in the chat-room, the training given and checking done on the backgrounds of the people who are employed by them as moderators. More information on staying safe in chat-rooms can be found on the Home Office site www.thinkuknow.co.uk .
- **Keep yourself informed:** Children may be exposed to risks because adults looking after them are unaware of the dangers they are confronted with.
- **Cyber-Bullying:** Remember cyber-bullying is a reality and our children may be subject to or may bully others via the internet. More information regarding this can be found at: http://stopcyberbullying.org/. **stopcyberbullyinh.org**

Advice to Children

Zip it

Never tell people online what school you go to, your home address or place stuff like your email details or mobile phone number on social network profiles.
Use a nickname in chat rooms and for instant messaging instead of your real name. Don’t give out your passwords, even to friends, to prevent yourself becoming a victim of cyber bullying.

Block it

Always delete emails from people you don't know and never open attachments or click on links unless you can be 100 per cent sure what they are. They could hide a virus. Learn how to block and delete anyone you come into contact with who makes you feel scared, worried, and uncomfortable or just doesn't seem right.

Flag it

If you don't feel you can talk to your carers about something encountered online, then speak to your social worker or another trusted adult. Or call free to Childline on 0800 1111.

Never meet anyone you only know in the online world. Just because they say they are a child or teenager, it doesn't mean they are.

Use some of the resources available via organisations such as CEOP to increase the awareness of children to enable them to safeguard themselves and regularly have discussions around E-Safety.

E-Safety Top Tips

- **Be involved in the child's online life.** For many of today's children there is no line between the online and offline worlds. Children use the internet to socialise and grow and, just as you guide and support them offline, you should be there for them online too. Talk to them about what they're doing, if they know you understand they are more likely to approach you if they need support.
- **Be educated in e-safety with knowledge.**
  The 'Thinkuknow' programme has films and advice for children from five all the way to 16. The child may have seen these at school, but they can also be a good tool for you to find out more about what children do online and some of the potential risks. Thinkuknow also provides information for parents and carers.
- **Keep up-to-date with child's development online.** Be inquisitive and interested in the new gadgets and sites that children are using. It's important that as they learn more, so do you.
- **Set boundaries in the online world just as you would in the real world.** Think about what they might see, what they share, who they talk to and how long they spend online. It is important to continue to discuss boundaries so that they evolve as their use of technology does.
- **Know what connects to the internet and how.** Nowadays even the TV connects to the internet. The child will use all sorts of devices and gadgets; make sure you're aware of which ones can connect to the internet, such as their phone or games console. Also, find out how they are accessing the internet – is it your connection or a neighbour's Wi-Fi? This will affect whether your safety settings are being applied.

- **Consider the use of parental controls on devices that link to the internet, such as the TV, laptops, computers, games consoles and mobile phones.** Parental controls are not just about locking and blocking, they are a tool to help you set appropriate boundaries as your child grows and develops. They are not the answer to a child's online safety, but they are a good start and are not as difficult to install as you might think. Service providers are working hard to make them simple, effective and user friendly. Find your service provider and learn how to set your controls
- **Emphasise that not everyone is who they say they are.** Make sure the child knows never to meet up with someone they only know online. People might not always be who they say they are. Make sure the child understands that they should never meet up with anyone they only know online without taking a trusted adult with them.
- **Know what to do if something goes wrong.** Just as in the offline world, you want to help the child when they need it. Therefore, it is important to know when and how to report any problem. What tools are there to help me keep a child safe?

Risks children face online

- Cyberbullying
- Virus's & hacking
- Grooming
- Overuse/addiction
- Online reputation
- Inappropriate websites
- Losing control over pictures and videos

What to do if you are worried about a child?

In all incidences, where it is believed or known that a child has been exposed to any online risk, residential staff must notify their line manager, Registered Manager and child's social worker. Depending on the nature of this concern the Registered Manager or social worker may make a referral to LADO (if this involves an adult known in a professional capacity to the child) or this may be reported to the police. Residential Staff are to ensure that they fully record/report their concerns and where appropriate screen shot/print off any offending material which may be used as evidence if this escalates to criminal charges being made. Please refer to the home's safeguarding policy and whistleblowing policy for further information.

Glossary of Terms

- **Chat-room:** A place on the internet accessed through a computer or mobile phone device, where people communicate by typing messages. People all over the world can communicate in a chart room, where everyone else can see what is being typed by anyone else, either on their computer screen or mobile device.
- **Cookie**: A piece of information sent by a Web server to a user's browser. Cookies may include information such as login or registration identification, user preferences, online "shopping cart" information, etc. The browser saves the information, and sends it back to the Web server whenever the browser returns to the Web site. The Web server may use the cookie to customize the display it sends to the user, or it may keep track of the different pages within the site that the user accesses. Browsers may be configured to alert the user when a cookie is being sent, or to refuse to accept cookies. Some sites, however, cannot be accessed unless the browser accepts cookies.
- **Data Mining or Online Profiling**: The practice of compiling information about Internet users by tracking their motions through Web sites, recording the time they spend there, what links they clink on and other details that the company desires, usually for marketing purposes.
- **Discussion group/Newsgroup**: Online area, like an electronic bulletin board, where users can read and add or "post" comments about a specific topic. Users can find discussion groups, also referred to as "discussion boards," for almost any topic.
- **Downloads**: Transfer of information on to a computer which often is free. It can be images, games, music etc.
- **File Sharing**: Accessing files on one computer from a different computer.
- **Filtering software**: Allows blocking out of certain material from the computer such as websites with violent, racist or sexual content.
- **Filtered ISP**: An Internet Service Provider (ISP) that sets criteria for determining content which is inappropriate for children, and automatically blocks subscriber access to that content.
- **Firewalls:** Are used to prevent unauthorised internet users from accessing private networks or individual computers connected to the internet. All messages entering or leaving the computer pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.
- **Flaming**: Posting or sending a deliberately confrontational message via news group, email, etc., usually in response to a previous message.
- **Instant Messaging (IM)**: Technology similar to that of chat rooms, which notifies a user when a friend is online, allowing them to "converse" by exchanging text messages.

- **ICQ:** Downloadable internet software that alerts someone to other people being online and allows contact to them. The software lets users chat, send messages and files, exchange web addresses and play games.
- **IRC**: Internet relay chat, which is another form of online chat with software that can be downloaded.
- **MMS**: Multi-media messaging service, which means sending messages between mobile phones or between mobile phones and computer email. These can be text messages, still images or short films.
- **Moderated chat room**: This is either an adult that is present or filtering software to make sure conversations taking place do not break the companies' policies about online behaviour.
- **Plug-in**: A small piece of software that enriches a larger piece of software by adding features or functions. Plug-in enabled browsers to play audio and video.
- **Spam:** Unsolicited "junk" email sent to large numbers of people to promote products or services. Sexually explicit unsolicited email is called "porn spam." Also refers to inappropriate promotional or commercial postings to discussion groups or bulletin boards.
- **Subscribe:** Means giving your email address to an organisation and they send information about themselves or their activities, events etc.
- **White list**: A list of 'good' email addresses or Web sites. Some filters are/can be configured to only accept email or allow access to Web sites from the White list. A White list can also be used to create exceptions to the rules that filter out "bad" addresses and sites.
- **Worm**: A program that reproduces itself over a network, usually performing malicious actions, such as using up the computers resources and possibly shutting the system down.

Useful resources and help

Advice.. Help.. Report..

CLICK CEOP

Visit ceop.police.uk

You can contact CEOP to ask for advice and guidance and also to make reports of concern.

http://www.ceop.police.uk/

Help from the Internet Watch Foundation (IWF)

If you have inadvertently stumbled across potentially illegal online content, specifically images of child sexual abuse, criminally obscene material or anything that incites racial hatred then please submit a report to the Internet Watch Foundation (IWF). The IWF works in partnership with the police, government, the online industry and the public to combat this type of material and you are helping to make the internet safer for all by taking this action.
Report to Internet Watch Foundation https://www.iwf.org.uk/report

Help from Child Line

ChildLine
0800 1111

Help from Cyber Mentors

Cyber mentors offer a very similar service online to Childline but this time you can speak to someone online who is your own age. Their site offers excellent advice and guidance so please use it. Visit the Cyber Mentors website

http://www.beatbullying.org/

Email: safeguardingpartnerships@warrington.gov.uk

Warrington Safeguarding Partnership can speak to parents, professionals and children and young people and provide information and advice.

Help from Action Fraud

If you have been 'scammed, ripped off or conned' you can report to Action Fraud, www.actionfraud.police.uk, or on 0300 1232040. It is a 24/7 service this service is run by the National Fraud Authority, the UK's government agency that helps coordinate the fight against fraud.

APPENDIX

An example of a young person internet agreement

E-Safety Agreement

Child:

- I agree to not give out personal information to anyone online, such as where I live.
- I agree to not access inappropriate web sites, such as anything over 18.
- I agree to not access or download, pornographic, prejudicial or extremist, drug/criminal related images/videos, information or material.
- I agree to be careful on social media with regards to what I post.
- I agree to provide staff with my passwords to all of my electronic devices.
- I agree to Staff checking my internet browser history, and downloads on a planned basis or unplanned if staff have any concerns.
- I agree to not purchase anything online unless I have permission from staff
- I understand that if I do not adhere to this agreement or if my actions using electronic devices with internet access cause me or another harm then I may lose my internet access from my electronic devices or will be only able to access the internet when I am fully supervised by a member of staff.

Signed Child …………………………………..

Date…………………………..

Signed Keyworker ………………………………………

Date …………………………..