Internet and Social Media Guidance

Code of Practice for Foster Carers

Version: 3.0
Date Issue: September 2016/Updated October 2019
Author: Jo Smith/Lesley Malley
Team: Fostering Services
Protective Marking: Internal

Contents

1. Introduction

1.1 This guidance is for use by staff in fostering services. It complies with the National Minimum Standards for Fostering Services and has been implemented to support foster carers in managing internet and social media safety.

1.2 The purpose of the guidance is to:

- keep young people safe;
- protect foster carers;
- ensure that foster carers do not inadvertently bring Warwickshire County Council into disrepute.

1.3 This guidance and code of conduct is underpinned by:

- The Byron Review Into child/young person and New Technology (2008);
- The Fostering Service Regulations (2011);
- Support, training and information for foster parents;
- The National Minimum Standards for Fostering Services (2011) 4.4 which states: “foster carers encourage children and young people to take appropriate rules as a normal part of growing up. Children and young people are helped to understand how to keep themselves safe including when outside of the household or when using the internet or social media”.

2. Children and young people’s access to the internet

2.1 For the purposes of accessing the rich source of information, entertainment and networking, children and young people should be encouraged to access the internet. However children and young people can be vulnerable to inappropriate materials, harassment and cyber bullying. Paedophiles also make use of the internet and new media to access vulnerable children/young people, gain their trust and groom them for abuse. Therefore, in order to ensure that children and young people are protected as far as possible:

- **Foster carers should take an active interest in child/young person’s activity online.** If foster carers don’t understand the internet they could ask child/young person to teach them. This may help foster carers to understand how it works and what children and young people are doing. Foster carers should ensure that they read the guidance and required material identified throughout this document.

- **Foster carers will need to work as a team with children and young people.** Boundaries should be set by foster carers. This involves discussing with the child/young person exactly what is acceptable and what is not regarding the kind of web sites that are appropriate for them to visit, which chat rooms to visit and what kind of subjects are acceptable or not to talk about on sites. Children and young people should be informed about the consequences of disregarding the agreed rules (e.g. being banned from using the internet for a short period of time), although foster carer's should not threaten to ban the use of the internet permanently. Children and young people can also access websites from mobile sources, for example their telephone, laptop, iPod, gaming devices or tablets or their friends. As such, foster carers should regularly monitor internet use on these devices, set times for use, check the settings and be aware how children and young people are using them. More information can be found about setting up parental controls on Warwickshire County Council's web pages under Cyber Safety.

- **It is important that the position of the computer** is fixed by foster carers in the main living space. Foster carers should ensure that the monitor faces OUTWARD into the room so there is no secrecy. This is one of the single most valuable things foster carers can do to ensure the safety of children and young people online. Foster carers should check whether parental controls are set as default on mobile phones and other mobile devices and whether the children and young people can restrict the ability to download some or all apps. If parental controls are not set by default, the foster carer should contact the mobile phone provider and arrange for them to be switched on.

- Free public Wi-Fi is available widely to children and young people. Technology known as the 'Friendly Wi-Fi 33' scheme is designed to identify public places such as shops, restaurants, cafes and cinemas, providing secure filtered Wi-Fi 33. Initiated by the UK Government with support from the UK Council for Child/young person Internet Safety (UKCCIS) and managed by the RDI trade organisation, the scheme means that children and young people, foster carers, parents and guardians can look for the Friendly Wi-Fi 33 logo and be confident that the public network has been tested and verified to make sure pornographic and children and young people abuse websites are blocked.

- **Children and young people should be encouraged to report** immediately to their foster carer any strange or upsetting messages they might get whilst chatting. Foster carer's should make it clear that they will not be angry with children and young people if this happens and that they will not ban their use of the internet as a result. It should be made clear to children and young people that they cannot control the things that other people say to them whilst they are chatting on the internet and that they are not to blame if this does happens.

- **Foster carers should set strict time limits** for internet chat room use by children and young people. Internet addiction is an issue for children and young people and foster carers should be aware of this and make use of and enforce these limits.

- **Foster carers should make it clear to the children and young people that people in chat rooms** are ALWAYS strangers, no matter how often they chat to them, and no matter how well they think they know them, and that while they may be good or bad people, they are still strangers.

- **Foster carers should make sure that if children and young people are using a social networking site they have** ensured privacy settings are set to “friends only” wherever possible and not to “recommend”.

- **Foster carers should make sure that the children and young people understand that they are never** to give out personal information online, such as their real name, their school, their phone number or where they live.

- **Foster carers should not permit the children and young people to be left alone** online, gaming for long periods of time as this is when they are most vulnerable. Foster carers will need to make sure that chat time occurs when they are present in the house so that they can check on children and young people regularly.

- **Foster carers must stress to the child/young person that they are to behave politely** and respectfully at all times while chatting online or sending email to friends.

- **Foster carers must be concerned if** the child/young person appears to be trying to prevent them from seeing the screen and gets defensive or insists/demands to be alone when chatting online. If foster carers hear the child/young person “clicking” on their computer mouse every time they approach, this might mean that the child/young person is closing or hiding a window, so that the foster carer cannot see what they are doing.

- **If helpful, the foster carer could** set up a written agreement with the child/young person around internet use. Alternatively the foster carer could involve the family and all children or young people placed in writing their own family code of “Acceptable Computer and Internet Use”

  Note: When following the above guidance foster carers must give consideration to what is appropriate for the child/young person placed and will need to take account of their age, ability, and their individual vulnerability.

3. Protecting the computer

3.1 Foster carers must ensure their computers are “protected to avoid damage to the computer, ‘pop ups’ and ‘spam’ or unwanted and inappropriate sites (including pornography) being uploading onto their computer uninvited. Foster carers need to ensure that any computer a child/young person may be using has anti-virus software, a firewall and anti-spyware installed to avoid computer damage or identify theft.

3.2 Foster carers should protect their password to ensure that a child/young person in their care or hackers cannot break it. This can be done by avoiding easy to guess passwords, e.g. pets names, birthday etc. that. Foster carers should also change passwords regularly.

3.3 Foster carers must secure their wireless network by:

- resetting the router password;
- enabling wireless encryption to prevent a stranger from seeing their network from the internet;
- restricting the access they share on the network;
- ensuring their network security software is kept up to date.

3.4 Anti-Virus Software

3.4.1 Viruses are more commonly spread via email, concealed within email attachments. However they can also be spread via downloadable games, demonstration copies of software on the internet, or files shared between individuals. Once a user opens a corrupted file, the virus is activated. Sometimes the damage caused is obvious, other times a delay occurs before the effect is seen. Effects range from being linked to an inappropriate website with adult content, installation of an unsuitable image for a computer’s screensaver, alteration or deletion of files, to copying itself to all individuals listed within an email address book.

3.4.2 Types of viruses include:

- **Virus:** a program that installs itself on a computer without the owner’s knowledge and often runs covertly in the background, often damaging files;
- **Worm:** a type of virus which replicates itself and is usually transmitted by email. Tends only be apparent after the computer system slows down;
- **Trojan:** a virus program that often sits benignly hidden until it is triggered by some event such as installing some software. The Trojan can deploy both viruses or worms and in some cases even take complete control of a computer.

3.4.3 Anti-virus software checks all incoming ‘traffic’ including web pages, email, attachments, instant messaging (IM) and downloaded files for signs of viruses. If detected by the software there is a good chance it will be stopped and destroyed before damaging a PC.

3.4.4 It is vital for foster carers to have up-to-date anti-virus software installed onto their PC. This must be installed before they connect their PC to the internet, and should be regularly updated to provide up-to-the-minute cover. Anti-virus software is usually licensed and should be set to update automatically. If foster carers use anti-virus software from their Internet Service Provider, it will check for updates and install automatically to the PC, when connecting to the internet. Other anti-virus software companies release updated files on a very regular basis to combat any newly detected viruses. It is vital that foster carers ensure their PC is always running with the latest anti-virus software updates.

3.5 Firewall

3.5.1 A firewall is simply a program (or hardware device) that filters information coming through the internet connection onto a PC - it acts like a barrier and keeps a list of ‘rules’ detailing what can and cannot pass between the PC and the internet. Therefore if certain information is ‘flagged’ by the firewall filters it will not be allowed through.

3.5.2 Foster carers are in control of establishing the ‘rules’ and security settings offered by the firewall, and can therefore determine what they want to block. The highest setting is to block everything, although obviously nothing will then get through. The best way is to block everything and then select what type of information foster carers wish to will allow e.g. email, a chat client, web browser information etc. The default settings provided by the firewall developer are strongly recommended unless foster carers have a specific reason to alter the settings.

3.5.3 Installing a firewall may protect an individual from gaining access to a PC and controlling it in some form – from viewing/accessing files on a PC to actually running programs for example e-mail bombs, which are hundreds or thousands of copies of the same email sent to an email address until the email system cannot accept any more messages; and/or application/bug backdoors whereby programs have features that allow for remote access to a PC.

3.5.4 A firewall is not 100% secure and does not guarantee full security and there are regular updates to all personal firewalls which should be automatically installed to fix bugs, correct problems and add extra protection.

3.6 Anti-Spyware

3.6.1 Anti- spyware will work in a similar way to anti-virus software, by providing active protection as well as detecting any spyware products on downloads.

3.6.2 Whilst spyware doesn't damage a PC in the way a virus would it can: generate endless pop-up advertisements that make the web browser slow and unusable; foster carers are advised to reset browsers to 'home redirect and control web searches conducted and modify their home icon.

3.6.3 Anti-spyware will protect a foster carer's identity from being compromised, detects persistent and offensive internet promotions, monitors the PC for changes in security settings and prevents unwanted programs reporting on internet activity. Anti-spyware software also needs to be updated regularly and is usually achieved via automatic updates.

3.6.4 Software packages are available to enable user monitoring which can be found at: www.getnetwise.org.These software packages can be used to:

- Control contents;
- Control contacts;
- Control shopping and privacy;
- Help with time management and health;
- Improve general security; and
- Monitor and record activity.

4. Internet and social media code of conduct for foster carers – managing information responsibly and fairly (Information Governance)

4.1 It is important when foster carers are using the internet that they are mindful of Warwickshire County Council's expectations in respect of confidentiality and data protection and do not exchange information over the internet in any way that contravenes these requirements. **Foster carers need to be aware that if they do so it will result in the procedure for** Dealing with Allegations, Complaints, and Causes for Concern against Foster Carers **as a minimum but could result in de-registration.**

4.2 Foster carers should also encourage and educate their own child/young person to respect the confidentiality of any children and young people placed and their families and to ensure their child/young person is aware of the issues around the internet and social networking sites. Foster carers must ensure their child/young person is aware of the expectation that they will not share information or photographs of children and young people in their care via the internet or through the use of other social media including mobile phones or the online use of X Box or its equivalent.

4.3 E-Mail

4.3.1 WeLearn365 has been developed by Microsoft and Warwickshire ICT as a portal to share emails and information in a secure way. It is a secure site and foster carers will have their own individual logins and access. We-Learn will also give foster carers the opportunity to complete on-line e-learning for a wide range of training courses.

4.3.2 There is increasing pressure on staff to use email to communicate externally to non "warwickshire.gov.uk" addresses. Unfortunately as the corporate 'email and Internet Code of Practice' points out this is as secure as sending confidential information on a postcard. The reason for this is that email copies reside on all servers through which they are transmitted, and each transmission can go through several servers. These are vulnerable to hacking. To ensure that emails are transmitted safely and securely, foster carers should familiarise themselves fully with the following guidance:

- Record Keeping for Foster Carers;
- WCC Information Security Policy;
- Data Protection Act 1998;
- Access to Records LOCAL Government Act 1974;
- The Children Act 1989 Guidance and Regulations, Vol 2 Care Planning; Placement and Case Review Chap 7:7:1 – 7:15;
- Information Governance Management Framework

4.4 Recording personal information

4.4.1 Foster carers should be careful about recording unguarded or casual opinions about individuals or their circumstances as factual which are not. They should remember that the subjects of the recording have legal rights to see information held about them, including comments made in emails.

4.4.2 Foster carers should not send a communication by email when they feel angry or upset. They should be aware that every email sent in respect of a child/young person will form part of the child/young person's records.

4.4.3 In addition foster carers should:

- Refrain from storing information on removable devices, CD's, DVD's, USB devices;
- Ensure that confidentiality is maintained at all times when transporting personal or confidential information. (they should not leave confidential documents on display in their car and they should ensure that laptops

have protection for personal data held on them and make sure that they are not left at risk of theft).

4.5 Social Networking Sites

4.5.1 Social networking sites have become part of social life and sharing with friends and family. Foster carers are in a unique position in that children and young people placed with them will be included on family photographs etc. For foster carers using these sites they need to be mindful of the following:

- Foster carers **must not** upload pictures of Looked After children and young people who they are caring for/or have cared for onto their personal social network pages. This is a breach of confidentiality regardless of whether a child/young person has consented. Foster carers also need to be mindful that parents of children and young people also use social networking sites and finding pictures of their child/young person on the internet could be distressing or harmful to some parents.

- Looked After young people can upload photographs onto their own social networking site pages and foster carers can support them to do this.

- When writing “blogs” or on “walls” foster carers **must not** write information about the Looked After children or young people placed with them. This could potentially cause distress to parents of children and young people who may access this information via the internet and could potentially compromise the safety of a child/young person. This is a breach of confidentiality.

- Foster carers must ensure that they have written evidence of consent to place images or written information on the internet relating to children or young people placed with them/previously placed with them.

- Foster carers also need to be mindful of any pictures they upload onto social networking sites. For example photographs of children in the bath or pictures of young children nude on the beach should be kept for personal memories only and not uploaded onto social networking sites. However, pictures of this nature must not be taken of Looked After children or young people under any circumstances. This is to ensure that foster carers do not find themselves the subject of media attention by virtue of their role and potentially bring Warwickshire County Council into disrepute.

- It is recommended that foster carers DO NOT allow children and young people currently or previously placed to become their “friends” on social networking sites. They need to ensure that there are no images on their pages or information on their “wall” which is “too adult” or could be interpreted as contravening Fostering Services National Minimum Standards. In exception circumstances, this can be agreed between the foster carer and the child/young person’s social worker but this agreement must be included in the placement plan.

- Foster carers should educate and encourage their own child/young person to respect the confidentiality of young people placed and their families.

- Where a foster carer becomes aware that another foster carer is breaching the above guidelines they are obligated to discuss this with their fostering social worker who will take any appropriate action.

- Children and young people who use Facebook and their carers are invited to add the new Child Exploitation and Online Protection Click (CEOP) 'app' to their profile. This application provides advice, help and support from the CEOP Centre. Crucially, children/young people will be able to report instances of suspected grooming or inappropriate sexual behaviour directly from their profile to specially trained investigators.

- Once added to their profiles, children/young people will receive regular messages from CEOP and its partner organisations about making children and young people safer. CEOP's new Facebook page will also contain polls, news alerts and status updates. The page will look at topics that teenagers care about, such as celebrities, music and exams and will link these subjects to questions about online safety.

- Children and young people can either add or bookmark the 'app' so it appears on their profile, as not only a constant source of help and reassurance for them but also as a strong visual signal to their friends, family and others that they are in control online.

4.6 Be Aware

4.6.1 Most mobile telephones have cameras. Foster carers should talk to children/young people about the need to protect photographs online from strangers or peers who may use them inappropriately. Photos held on mobiles and/or networking sites or webcams can be copied, recorded, shared and ultimately end up anywhere.

4.6.2 Sexting is where pictures, videos or messages of a sexual nature are sent from one mobile to another. Sexting can be linked to child sexual exploitation.

4.6.3 Cyber bullying and cyber stalking is becoming more common. It is the use of email, instant messaging (IM) and mobile phone messages or photos to embarrass or bully children and young people. If this happens, foster carers must keep a copy of any bullying messages by using 'print screen' on their computer keyboard.

4.6.4 Online self-harm, self-trolling or self-cyber bullying is when children/young people set up multiple profiles in different names and use them to post abusive messages to themselves.

4.6.5 Foster carers must be vigilant to the use of sites for gambling, racism, anorexia and hate sites and if they discover a child/young person using these sites, they must inform the child/young person's social worker.

4.7 Other Social Media

4.7 Technology moves faster than many of us can keep up with whether it is mobile phones, IPhone, IPad, Xbox, PlayStation, or their equivalent. The form of social media is not what is important it is the principle as carers and as a foster family of not breaching confidentiality and remembering the distress that can be caused to children and young people Looked After and their families in the event this occurs.

4.8 The principles above must be applied to all social media and does not just apply to standard computer internet use.

5. Further Information

See Social Media: Corporate Policies and Guidance

It is advised that this guidance is read in conjunction with:

- Warwickshire's e-Safety Advice for Parents and Carers;
- A Parent's Guide to Facebook

- Other excellent sites for all aspects of internet safety remain; www.childnet.com, www.childnet.com/kia,
- www.digizen.org,
- www.ico.org.uk, www.iwf.org.uk,
- www.ceop.police.uk,
- www.thinkuknow.co.uk,
- www.respectyourself.info,
- www.childline.org.uk, www.commomsensemedia,org

Additionally Warwickshire Fostering, Central Recruitment and Training team offer an excellent course called Internet Security and Privacy which is updated to ensure it keeps pace with changes to the internet.