Girlguiding

A Safe Cyberspace

Making the most of digital tools in guiding

November 2014

Contents

Introduction

The internet and social media provide fantastic opportunities to give girls a voice. Our young members and adult volunteers alike use these great tools to socialise, communicate and learn, and also to speak out positively about issues that matter to them.

However, there are risks in the online world just as there are offline, including exposure to offensive material, cyberbullying, trolling, harassment and grooming.

Our online safety guidance is intended to help safeguard our members by supporting adult volunteers to deal with the issues that may arise, and encouraging good practice when using the internet. These guidelines should also be shared with young members to ensure that they know how to be safe online.

> **Note: 'Volunteer' refers to both members and recognised volunteers within Girlguiding.**

Digital communication policy

- You should not contact members under the age of 14 directly. Communication should be with parents/carers and always from a member of the Leadership Team.
- When contacting parents/carers or young members over the age of 14, you should:
  - use appropriate language – try to avoid any words or phrases that could be misinterpreted or misconstrued
  - ensure that any images you send are appropriate and that external hyperlinks you include do not lead to inappropriate content
  - copy another member of the Leadership Team into any message you send to a young member.
- Individual texting between girls and members of the Leadership Team is discouraged.

Linking policy

The Girlguiding website and our Facebook and Twitter feeds link to other websites and social media channels to inform and inspire our users. We take responsibility for content that is one click from our site – that it is fully checked, accurate and appropriate at the time of linking. If you find inappropriate content is being linked to from our site please let us know at **concerns@girlguiding. org.uk**. Content that is more than one click away from our site is more difficult to monitor. However, we would like to know if you find inappropriate content related to Girlguiding online.

A safe cyberspace for volunteers

We want to encourage you to join us in making the most of social media to share your guiding story. The guidance in this document will help you. It might seem daunting at first, but there really isn't anything to be worried about.

The opportunities for volunteers on social media are huge! For example, you can:

- share pictures and information about your unit's activities and events
- promote your unit to potential new volunteers
- share what girls in your unit have been up to with their parents and wider families
- build relationships with influential people in your area
- connect with Girlguiding volunteers and Leaders across the UK and the wider world
- share best practice with other Leaders and find out what works well for them.

Many unit meeting places do not have internet access, but you can make use of smartphones or tablets. Alternatively, you can take photos or videos in the unit meeting and share these when you are home.

If you would like more information on how to get up and running with social media, the platforms themselves can be the best place to start.

- **https://support.twitter.com** > Welcome to Twitter > Getting started with Twitter.
- **https://www.facebook.com/help** > Get started on Facebook.

You can also check out pages 7 and 8 of this document for a summary of the most popular sites and a glossary of terms.

> **At all times, Girlguiding aims to ensure that the right safeguarding measures are in place to reduce any potential personal distress or risk to our reputation. As a Girlguiding volunteer, you are in a position of trust and you should interact with young members online in the same way as you would in person. All adult volunteers are expected to adhere to Girlguiding's Code of Conduct both online and offline.**
>
> **It is important to be aware of potential risks and online safety issues, and know the safety measures that should be put in place when interacting with others online. Think about the things that you post before uploading any content. Could the message be misinterpreted or could someone take offence? Could this bring Girlguiding into disrepute?**
>
> **Make sure you follow the ensuing guidelines, particularly those which relate to sharing information and photos/videos online.**

Unit websites/social networking groups

- Use Girlguiding's branding guidelines to help you apply our brand correctly on your unit website or social networking group (**www.girlguiding.org.uk** > Members' area > Resource library > Our brand).
- Ensure that the Leadership Team and meeting place owners have given consent for information regarding unit meeting times, dates and location to be shared, including any contact details.

- Provide a link to Join Us (www.girlguiding.org.uk/interested) for any membership enquiries.
- If you have used any images from another website, make sure you have permission from the website owner or copyright holder. For any text, reference the source.
- If you are setting up a social networking group on Facebook for girls from your unit/District, make sure it is a 'closed' group. If a group is 'open', there is no guarantee that all members will be genuine members of Girlguiding. There are a number of open groups that have not been officially endorsed by Girlguiding.
- For a social networking group, a minimum of two administrators should moderate interaction and ensure that appropriate communication takes place between each administrator and group members. Remember that you do not have to be 'friends' on Facebook to invite someone to join a group.
- When accepting young members into a group, ensure that the content of the group is appropriate and relevant for their age.
- Creating website/social networking group codes of conduct can encourage young members and adult volunteers to be respectful online.

Photo/video permissions

We want to show people all the exciting events and activities that guiding brings to girls and young women, so it's only natural to take photos and/or videos. Girlguiding offers the following permissions on the Starting… form for each section to help girls and their parents take control of how their images are used.

- ○ I am happy for photographs/videos to be taken of my daughter during guiding activities and used in national and local guiding publicity, communications, publications or digital channels (eg websites, social media)
- ○ I am happy for photographs/videos to be taken of my daughter during guiding activities for use within the unit only, **not used** for national and local guiding publicity, communications, publications or digital channels (eg websites, social media)
- ○ I do not wish any photographs/videos to be taken of my daughter while she undertakes guiding activities.

> **Please note that photo/video permissions differ for large-scale events (where over 100 participants are present). Consent forms will state clearly if an event is large scale, and will request you to make it known to your daughter's Leader if you do not wish photos/videos of her to be taken at the event.**

Sharing photos and/or videos

- Ensure that you have checked parental permission before sharing photos or videos of young members on websites, social networking sites or specialist media-sharing sites such as YouTube.
- Avoid mentioning members' full names or including other information that could reveal their identities. Be aware that members' full names will be visible on

Facebook and Twitter, so think carefully about the content you are posting.
- Make sure girls are aware that they should not share photos or videos of their friends online without permission from parents/carers.
- Consider disabling the ability to comment on YouTube videos. This is a great interactive feature, but it also allows users to post negative comments or abuse.

Email

- Ensure that appropriate email addresses are used when communicating in a guiding capacity. Your guiding and personal email accounts should be separate.
- Use the Bcc (blind carbon copy) box when emailing a group of people – this will ensure you don't share anyone's contact details without their permission and protect everyone against spam.
- Do not forward chain emails to young members or other adult volunteers.

> **If you receive an email from a young member that causes you concern, speak to your Commissioner and refer to *A Safe Space*. Find it at www.girlguiding.org.uk > Members' area > Running your unit > Child protection.**

A safe cyberspace for young members

Many girls and young women have grown up as 'digital natives', so you won't need to convince them of the many uses for digital technology. They will already go online to connect with friends and family, follow celebrities and get help with schoolwork. But you could encourage them to use their digital skills in their guiding lives. They might not have thought of all the possibilities.

1. Share pictures of activities in your unit on Instagram and Pinterest.
2. Make a photo or video diary of an event or camp using Instagram, Vine or YouTube.
3. Track an overseas trip on Wordpress or Tumblr to keep your friends and family in the loop.
4. Make a presentation for a badge clause using Prezi and share it online.
5. Use sites like Change.org and social media like Twitter to campaign on the issues you care about (see *Go For It! Be the change* at www.girlguiding.org.uk/guides > Badges and Go For Its! > Go For Its!).
6. Fundraise for your unit online using JustGiving, with regular updates of your progress.
7. Try making a simple online game for Rainbows to play using Scratch coding.
8. Hold a brainstorm in your unit meeting to come up with even more ideas!

It is essential to make your Rainbows, Brownies, Guides and members of The Senior Section aware of the potential risks to interacting online and how they can stay safe. Keeping up to date with digital technology is the best way to look after girls and young women online, and this document is a great starting point for some open and honest conversations about online safety.

Age restrictions

Many social networking sites have minimum age requirements for joining. Please ensure that young members are aware of this.

Sometimes, young people will use social networking sites at a younger age than is recommended, so we must offer them a safe space to talk about their online interactions.

Social networking profiles

- It is important for young members to think carefully about what information they disclose on their profile pages and choose display pictures wisely. Is it suitable for others to see?
- Young members should think about the things they are posting in the same way that adults should. Could the message be misinterpreted, offensive or considered a form of bullying? If they are unsure, advise them to ask another person to check the post first.
- If a young member is contacted by another user, they should not provide any personal details such as name, address, telephone number or the school that they attend, nor should they ask for another user's personal details. Can they be sure another user is who they say they are?
- Where possible, girls should look out for their friends too and tell a trusted adult if they are worried about something they see online. Visit www.thinkuknow.co.uk for further information and advice.
- Remind young members that what they post online may be viewed by their school, college, university or future employer.

Photos/videos

Remind young members that once a photo is posted online, they lose control of it. Girls need to think carefully about whether the image is appropriate to post. Ask them to think about whether they might be upset if someone sees it that they didn't think would see it.

Passwords

Tell girls to keep their login details and passwords safe and secure. They should not share this information with anyone else.

Privacy settings

Privacy settings will vary between different social networking sites, and can change over time. Things they thought were hidden might become visible to friends or other users, so members should check their settings regularly for each of the sites they use.

Accepting and meeting 'friends'

Young members may be contacted on social media by people they don't know, and some may request to add them as a 'friend' or 'contact'. Emphasise to young members that they should only accept people they actually know as friends, and remind them that they can always block or delete a contact if necessary.

Ensure that girls are aware that people they meet online are strangers and they should not meet up with them. If they do decide to meet someone they have met online, they must tell a parent/carer who can go with them.

Private inbox messaging

Remind young members not to respond to private inbox messages unless they actually know the sender. If they do receive a private inbox message from someone they don't know and decide they would like to reply, they should make a trusted adult aware of this communication.

Adverts and spam

Advise girls that spam (irrelevant or unsolicited messages) or adverts such as pop-ups which encourage them to visit a website can actually mask computer viruses. Ensure young members are aware that computers have security features such as firewalls, anti-spyware or anti-virus and they should speak to their parent/carer about these features. They can also turn on pop-up blockers.

Webcams

Young members should be very cautious when using webcams and only do so with people they actually know and see in everyday life, such as friends or family. It is important to make young members aware that when they use a webcam the image can be recorded, copied and shared without them knowing.

Unwanted images

Young members may see or receive an unwanted image, or have an image of them shared without their consent. Encourage girls to tell a trusted adult as soon as possible if this happens, and reassure them that it is not their fault. You can contact the service provider (eg Facebook) to have an image removed and, if you feel it is necessary, you can also report it to the Child Exploitation and Online Protection Centre (CEOP) through its online reporting form. Visit http://ceop.police.uk/safety-centre for more information.

Viewing adult content

Young people may come across adult material of a sexual nature. The adult material being circulated online is increasingly violent and creates an expectation for young people to perform or look a certain way. You can contact the service provider (eg Facebook) to have an image removed and, if you feel it is necessary, you can also report it to the Child Exploitation and Online Protection Centre (CEOP) through its online reporting form. Visit http://ceop.police.uk/safety-centre for more information.

It is important to challenge the representations seen online and to educate young members about real sex and relationships. Our Free Being Me programme

provides an opportunity for young members to challenge societal pressures and perceptions and to increase their confidence and self-esteem.

Sexting

Sexting refers to making or sending self-generated inappropriate or explicit material (including photos) of a sexual nature.

Remind young members that photos are easy to forward, copy, edit and post online without their knowledge or consent. Young members should be made aware of the consequences of sexting if this is shared outside of the intended recipient and that they can be supported if any material is shared that upsets them. Try to provide advice and guidance so that young members can make an informed choice about how they share and distribute photos.

Childline's ZipIt app is a friendly flirting app to defuse the pressure to 'sext' with tips and advice on flirting that enable young people to stay in control. More information can be found at www.childline.org.uk/play/getinvolved/pages/sexting-zipit-app.aspx.

Cyberbullying

Cyberbullying can occur via email, social networking and gaming sites, online chat or text message.

Encourage young members not to respond if they receive threatening or abusive messages. Instead, they should save the messages and keep a copy – they can copy and paste the text or use the 'Print Screen' button on their keyboard and then save it in a document (in a programme such as Word or Paint) to show a trusted adult. Ensure girls are aware that when chatting online, most services allow you to block and report users.

Remind young members that if they find themselves in an unpleasant situation they should leave the website. They can always log out of their social networking profile if they are not happy with any content or comments that they receive or see. They can also temporarily deactivate their account if necessary.

If a young member is receiving hurtful messages via their mobile phone, they should not reply. Advise them not to answer calls from a withheld number. They can speak to their mobile network provider about barring contact from a certain number. However, some mobile phone operators will take action only if the police are involved. Alternatively, they could think about changing their mobile phone number.

Always encourage young members to tell a trusted adult if they feel they are experiencing cyber-bullying. Attempting to deal with the situation alone may cause personal distress and the situation may escalate. Reassure girls that they are not at fault if this happens to them. If a young member feels they can't tell anyone, they can call ChildLine on 0800 1111 for support and advice.

Reporting a concern

Websites such as Twitter, Facebook, YouTube, Tumblr and Skype have their own policies and rules about what is deemed appropriate content. Each website has its own reporting methods, and you should contact the service provider directly to report your concerns.

If someone online has acted inappropriately towards you, a young member or someone you know, you can also report it directly to the Child Exploitation and Online Protection Centre (CEOP) through its online reporting form. Visit http://ceop.police.uk/safety-centre for more information.

What advice and support is available?

- **The Child Exploitation and Online Protection Centre (CEOP) command** is part of the National Crime Agency dedicated to eradicating the sexual abuse and exploitation of children. CEOP provides an online reporting facility for inappropriate content and images in relation to children and young people at http://ceop.police.uk/safety-centre. They also provide educational resources at www.thinkuknow.co.uk.

- **Childnet International** aims to help make the internet a great and safe place for children and young people by providing resources, support and education about services available online. Find the latest information on the sites and services that you like to use, plus information about mobiles, gaming, downloading and social networking at www.childnet-int.org.

- **ChildLine** provides great direct support for young people. It is a free, confidential helpline and you can call 24 hours a day on 0800 1111 to talk about a range of issues from bullying to relationships. Alternatively, you can visit www.childline.org.uk.

- **Kidscape** offers support for young people to tackle bullying. Find out more at www.kidscape.org.uk.

- **Girlguiding youth section web safe codes** provide age-appropriate online safety guidelines for our young members.
  - Rainbow web safe code – www.girlguiding.org.uk/rainbows > Web Safe Code.
  - Brownie web safe code – www.girlguiding.org.uk/brownies > Web Safe Code.
  - Guide web safe code – www.girlguiding.org.uk/guides > News and events > Guide web safe code.
  - The Senior Section web safe code – www.girlguiding.org.uk/theseniorsection > Resources > Web safe code.

Remember: Always consult *A Safe Space*. Download a copy from www.girlguiding.org.uk > Members' area > Running your unit > Safety > Child Protection.

Digital tools

Here are a few examples of the websites and digital tools you may hear young members mention.

Facebook

Facebook is an online social networking service where users can share updates, photos and videos and send 'friend' requests. Private messages and instant messaging are also available and you can 'tag' your location or friends along with the content you are sharing.

Facebook's Help Centre provides advice on managing your account, privacy and security settings, and reporting procedures. Visit https://www.facebook.com/help/ for more information.

Twitter

Twitter users send and read 140-character text messages called 'tweets'. Hashtags (like #guiding) can be added to tweets making it easier to follow conversations on specific topics. This makes Twitter an excellent tool for engaging people in a live event if they are unable to attend.

Twitter's Help Centre provides advice on getting started, using Twitter on your mobile, safety and security settings, and reporting procedures. Visit https://support.twitter.com/ for more information.

Blogging

A blog is an online personal journal that is regularly updated with new material about activities and interests. WordPress and Tumblr are two examples of free blogging platforms.

Blogging sites are usually set up as public viewing and blogs are a great way to share thoughts and experiences in a public space. It is important to encourage open conversations about the views that are being shared.

Skype

Skype enables users to make free audio and video calls including instant messaging. Other services are also available (such as calling mobiles from your computer), but may involve a charge.

Skype offers support and help with adding contacts, checking if your microphone, speakers and camera are working, and blocking unwanted users at https://support.skype.com/en/.

WhatsApp

WhatsApp is a platform to send and receive instant messages (including photos) on smartphones. It creates an account using your mobile phone number and you can change your username and photo.

Snapchat

Snapchat is a photo and video messaging service to share moments with your friends known as 'snaps'. Photos or videos shared with any of your contacts disappear after a few seconds, but the recipient can capture a screenshot of any image received.

For safety tips on Snapchat, try ConnectSafely's *A Parent's Guide to Snapchat*. Visit www.connectsafely.org > Guides.

YouTube

YouTube is a video-sharing website. Users are able to discover, watch and share videos.

YouTube's Help Centre has advice on creating and managing channels, paid content on YouTube, and policies, safety and reporting. Visit https://support.google.com/youtube for more information.

Instagram

Instagram is an online photo-sharing, video-sharing and social networking service. Users can take photos, apply filters to manipulate the image and then share them. Instagram is set as a default to public viewing, but you can change your account settings to 'private'. You can also tag other users in your photos, 'like' photos/videos and leave comments.

Instagram's Help Centre provides advice on privacy, discovering what's new and sharing photos safely. Visit https://help.instagram.com/ for more information.

For more safety tips, see ConnectSafely.org's *A Parent's Guide to Snapchat*. Visit www.connectsafely.org > Guides.

Vine

Vine is a social network and app that allows you to shoot and share short looping videos of up to six seconds, called Vines, from your phone or tablet device. Videos can be posted to specific channels such as Family and Fun, and they can be hashtagged to help people find videos on certain topics. Users can also be tagged in Vines.

Vine is closely integrated with Twitter. Some people build networks on Vine, while other people use Vine as an application for sharing their short videos on Twitter. Like Twitter, Vine allows you to 'follow' other accounts, and to be 'followed'.

For frequently asked questions about Vine, please visit https://support.twitter.com > Mobile & Apps > Vine.

Keek

Keek is a social network that allows you to shoot and share videos of up to 36 seconds, called Keeks, from your phone or tablet device. You can follow other accounts, and send and receive private video and text messages. Keeks can also be hashtagged, and users can be tagged using the @ symbol. Keeks can easily be shared to other social networks such as Facebook, Twitter and Tumblr.

For general queries about Keek, visit https://www.keek.com/faq.

Pinterest

On Pinterest, users can create 'boards', often themed, and can 'pin' images to them. People use it to collect ideas for their different projects and interests.

Pinterest's Help Centre provides advice on account security, reporting and how to activate or deactivate an account. Visit **http://help.pinterest.com/en** for more information.

Definitions

General

Avatar – An image that represents a person or organisation in an online community. Guiding accounts will use guiding branding as avatars, but you will also come across any number of different images or graphics that the account owner feels represents them, from cartoon cats to pictures of their favourite pop band.

Emoticon – An icon that shows emotion, such as a happy :) or sad :(face, which can be used to flavour your posts.

Smartphone – A mobile phone that provides a wide range of communication channels, such as social networking or video calling.

Spam – Unsolicited messages. These will often be promotional or may link to websites that try to infect your device with malware/viruses.

Troll – A person who attempts to derail an online conversation or who deliberately tries to enrage or bully people online by posting off-topic, rude or offensive posts or material.

Twitter

Direct message/DM – A private message sent to an individual user on Twitter.

Follower – A person that 'follows' a Twitter account. Tweets from the accounts that people follow will show up on their Twitter homescreen.

Handle – A Twitter username, for example @Girlguiding.

Hashtag – A way of following conversations on specific topics. Hashtags can be added to tweets by using the '#' symbol at the start of a word (eg #WorldThinkingDay).

Re-tweet/RT – Reposting a message posted by someone else.

Trending – When a phrase or a hashtag is used that attracts a large number of tweets over a short space of time it is said to be 'trending'. Recurring trends include the #FF or #FollowFriday hashtag, which people use to recommend people that they follow to their own followers.

Tweet – A public message posted on Twitter.

Facebook

Friend – Somebody you share updates with and receive updates from.

Group – Groups can provide a space for you to share updates with a small number of people. Groups can be set to:

- open (public) – anyone can see the group and what members post
- closed – anyone can see the group, but only members can see what has been posted
- secret – only members can see the group and posts.

Like – 'Likes' are used to follow pages (by 'liking' them), or to approve of posts and content.

Page – Used by brands. People can choose to 'Like' a page to receive updates.

Profile – Your personal Facebook presence.

Tag – To label a photo with someone's name.

Timeline – Facebook's way of presenting your profile. It shows your interactions and important milestones.

Common abbreviations

A/S/L – what is your age, sex and location?

ATM – at the moment

B/C – because

BRB – be right back

BBL – be back later

CU – see you

DIKU – do I know you?

DM – direct message

G2G – I've got to go

IM – instant message

IMO – in my opinion

IRL – in real life

L8R – later

LOL – laughing out loud

PIR – parent in the room

PM – private message

RT – re-tweet

SMH – shaking my head

TBH – to be honest

TTYL – talk to you later

WAYD – what are you doing?