



World Association
of Girl Guides
and Girl Scouts

Association mondiale
des Guides et des
Eclaireuses

Asociación
Mundial de las
Guías Scouts



**SURF
SMART**
STAYING SAFE ONLINE

"It took radio broadcasters 38 years to reach an audience of 50 million, television 13 years, and the Internet just 4."

This curriculum has been made possible in part by a grant from the Symantec Foundation, a corporate advised fund of Silicon Valley Community Foundation.

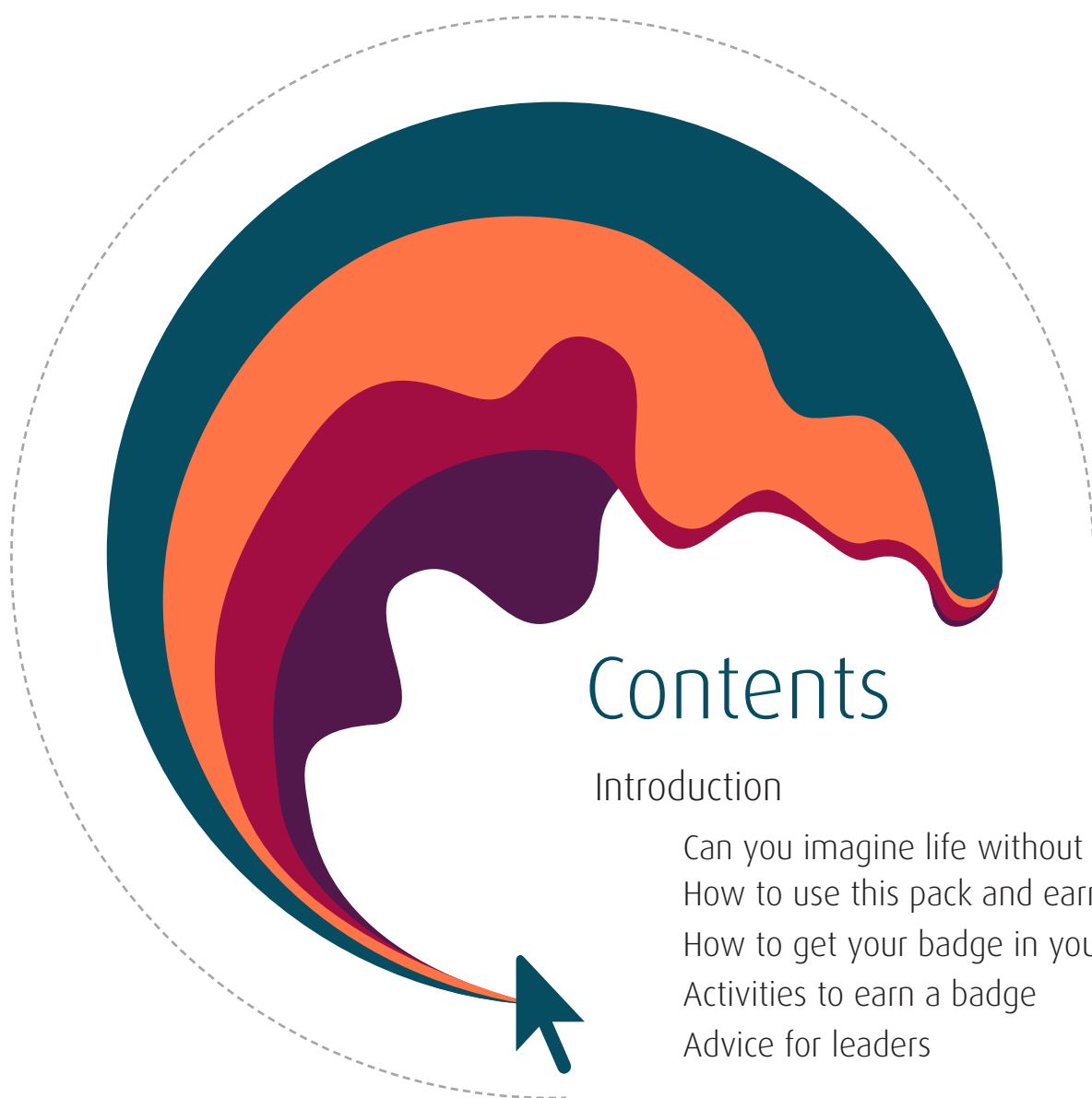
Written by Andii Verhoeven and with technical input from Marian Merritt
Edited by Nefeli Themeli & Timothy Findlay
Designed by Andriana Nassou

2nd edition
© WAGGGS, 2015

World Association of Girl Guides and Girl Scouts
World Bureau
12c Lyndhurst Road
London NW35PQ, England

Telephone: +44 (0)20 7794 1181
Facsimile: +44 (0)20 7431 3764
Email: wagggs@wagggs.org
www.wagggs.org

Registered Charity No. 1159255 in England and Wales



Contents

| | |
|---|----|
| Introduction | 5 |
| Can you imagine life without the internet? | 5 |
| How to use this pack and earn a badge | 5 |
| How to get your badge in your country | 5 |
| Activities to earn a badge | 5 |
| Advice for leaders | 6 |
| Connect...positively online | 8 |
| Protect...yourself from online risks | 17 |
| Respect...your rights and reputation online | 25 |
| Put yourself first | 34 |
| Adult internet safety guidelines | 36 |
| Email policy | 36 |
| Social network policy | 36 |
| General security online | 37 |
| Protecting group members | 37 |
| Resources and links | 38 |
| Internet Safety | 38 |
| Learning Opportunities | 38 |
| Glossary | 39 |

Introduction

Can you imagine life without the internet?

In 2014, the world's internet population reached 3 billion for the first time, equal to almost 40% of the people on the planet. As technology develops we are finding ever new ways to integrate the internet into our lives and it is predicted that by 2020, there will be 7 times as many devices connected to the internet as people on the planet.

The World Association of Girl Guides and Girl Scouts (WAGGGS) recognises the importance of the internet to our lives and also the vast opportunities it offers to our members. A Girl Guide in Peru or Kenya can now connect with a new friend in Canada, South Korea or India, bringing the Movement closer together than ever before and enabling girls and young women to connect together, to share information and to advocate on issues that are important to them in their communities, country and the world.

With such widespread use of this technology, it becomes more important than ever to ensure that our members can continue to use the internet safely, connecting positively with others online and respecting their own rights and reputation in the digital world. As with all risks, we believe it is important to work with girls and young women to support them to build their knowledge and understanding; providing opportunities through which they can equip themselves with the skills they will need to enjoy using internet technology safely and to its fullest potential and to build skills, awareness and confidence in managing the risks associated with it.

By partnering with Symantec, one of the largest internet security firms in the world, to produce this curriculum, WAGGGS hope to share with our members the company's expertise in online safety. With the professional support and advice of Symantec's cyber-security professionals and activities from WAGGGS non-formal education experts, we believe that the Surf Smart curriculum provides a unique resource which will ensure a generation of girls and young women are equipped with the skills required to protect themselves and others online.



Happy surfing!

Nicola Grinstead

How to use this pack and earn a badge

Just over 40 per cent of the world's population has access to the internet. If you're connected, the internet probably plays a big part in your life. You use it to answer questions, share with your friends and enjoy your spare time. Surf Smart takes you on a digital adventure to explore how to get more out of your time online and connect with local and global communities, and how to stay safe and make good choices when you're connected.



Surf Smart contains lots of fun activities to help you develop new digital skills and awareness. It has three themes:

Connect positively online (p. 8)

Protect yourself from online risks (p. 17)

Respect your rights and reputation online (p. 25)

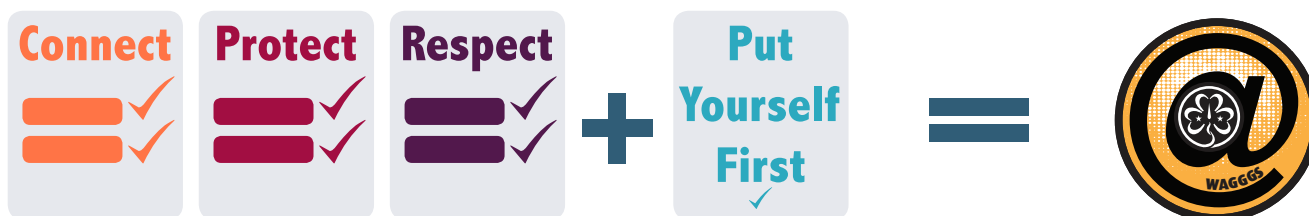
Look out for interesting extra facts to help you complete the activities and top tips to get the most out of your time online. As you work through the pack you may find words that are new to you; these are explained in the glossary on page 39.

How to get your badge in your country

When you complete the curriculum, you will need to receive your Surf Smart badge. The best way to do this is to contact your local organisation at the address below and they will be able to send this to you and your group.

Activities to earn a badge

Choose two activities from each theme (Connect – Protect – Respect) plus the activity “Put Yourself First” on page 34 to earn your badge.



Advice for leaders

- Internet safety is a growing issue as young people find more ways to make it part of their daily lives. This pack aims to raise awareness of internet safety for as many Guides and Scouts as possible. You can help by adapting the activities and badge requirements to make Surf Smart accessible for your members – you know them best!
- The activities in this pack have been developed for WAGGGS members of all ages and both genders, and with input from a range of countries. Some activities have been marked as more suitable for older or younger members but please use your own judgement when selecting activities for your group. Although it is important for our members to be aware of how to stay safe in any online situation, Surf Smart encourages, but does not push members to go online and can be used in environments without internet access.
- The suggested times for each activity are a guide to help you with your planning. They depend on the size of your group and how much you are adapting the activities.
- Please explore the information in this pack before starting the activities. Throughout the pack there are 'info boxes' that provide the necessary information you need to share with the youth members before, during or after each activity. The online links we've chosen are considered appropriate for a youth audience but we advise you to check them in advance to be sure you are happy sharing them with your group.
- We recommend that activities requiring online time be restricted to members of 13 years and older. This is because some commonly used online services such as Facebook and YouTube are not intended for children under 13. However, this is only a guideline and you may consider many of these activities appropriate for younger members. As children are now learning to use the internet as soon as they start school, if not earlier, we feel it's important our members start learning about internet safety as soon as possible.
- It is your responsibility to ensure that all appropriate safeguards are in place, and consents obtained, when using this resource. Please make use of the adult internet safety guidelines on page 36 to support this.
- We encourage you to add any relevant content you discover in your own research. You'll find videos, music, photos, games and plenty of information on YouTube and the websites listed at the back of the pack.

Share!

Finally, it would be great to share your Surf Smart experience, the photos you took and videos you created with Guides and Scouts from around the world!

There are lots of ways to connect with WAGGGS!



Visit www.waggggs.org



Twitter (@waggggs_world)



Facebook
(www.facebook.com/waggggs)



Tell us what you think about the activity pack by completing an online survey:
www.waggggs.org/en/internetsafety



Email your Surf Smart story to
youthlearning@waggggs.org



LET'S
START

Connect...positively online

Complete any two activities to earn your badge!

TIP!

Look out for your friends online; if you think they are at risk, take action!



1 What it means for me

The internet has become a big part of our lives very quickly. Make a list of the ways you feel the internet affects your life, both positively and negatively. Ask people you know from a different generation, such as parents and grandparents, how they use the internet in their daily lives. How are their answers different to yours? Create a display of the answers using posters, leaflets, blog posts or videos.



15 mins



paper, pencil, colour pencils for all participants

ALL AGES

Take it further – Choose someone from an earlier generation who you think has changed the world such as Emmeline Pankhurst, Mahatma Gandhi, Rosa Parks or Nelson Mandela. What do you think they would have done differently if they'd had a social network account?



10 min



Social networks

Social networks are a big part of online life. They make it really easy to keep in touch with your friends and explore lots of new content like videos, photos and chat all on the same web service.

- Check your privacy settings and ask a friend or family member to look at your profile to make sure you're not posting information you'd rather not display. When you look at your social network every day, it's very easy to miss simple things that it might be better to keep to yourself.
- Read up on digital reputation and creating for the internet as these topics are really important when you're using social networks.
- If you're under 13, you're not supposed to have a Facebook account.
- If someone asks to be your online 'friend', don't just automatically click "yes". Do you really know the person? If not, think about whether you want them to be able to see your profile and posts.



2 Short or long?

Give everyone three objects to include in a story. Half the group should invent a story of any length. Half the group can only use 140 characters to write their story. Share the stories. Which group found it easiest to tell a good story?



10 mins



paper, pencil, 3 objects



Take it further – Short social network posts can make it hard to get your message across. Using your group account try sharing your story using different social media such as Facebook, twitter, Google+, tumblr, VK, etc. What kind of messages do you think work well on social networks? Are there other messages it's better to share in different ways?



10min



computer/tablet/smartphone
with internet access



3 What's the message?

Give everyone a slip of paper and sit in a circle. The first person whispers a word to their neighbour, who draws a picture of what they hear and passes it to the third person, who whispers what they see to the next person and so on with the message alternating between words and pictures. Is the message the same when it gets back to the beginning? Start with simple objects or phrases then make the message more complex. Ask your leader to secretly select someone in the circle who will change one word of the message. Can you work out where it changed?

Discuss: How can messages change online? When you've posted information online, how much control do you have over it?



10 mins



paper, pencil

ALL AGES

Nearly **40%**

of the global population uses the internet

4 Get connected

The internet is not the only way for people to connect. As a Guide & Scout, you are part of a worldwide Movement that brings together young people from 146 countries. Research different ways of getting in touch with a Guide & Scout group in another country or with one of WAGGGS' World Centres. Show your plans to your leader then try them out together. Methods include email, online phone, video calling, and sending a letter to a group you found online. Being in touch with people from another culture is very exciting but it's important to understand and respect the differences between your lives. This is just as true when you connect through the internet as it would be if you met face-to-face. Research their society and culture and practice asking non-judgmental questions to learn more about their lives. If you're connecting in real time, don't forget to take into account the time difference.



20 mins



computer/tablet/smartphone with internet access, paper, pencil



Take it further – Set up a SKYPE account for your group and make contact with different WAGGGS members this way.

Please visit: www.wagggs.org/en/internetsafety for more information on how to connect



20 min



computer/tablet/smartphone with internet access



5 Go local

It's not just about worldwide connections; the internet can be a great way of getting in touch with your local community and sharing opportunities. But what happens if you can't find the facts you need? Research your community's online presence – could it be better? Find out about the opportunities available to young people in your community and research how you could use an internet portal, such as a website or Facebook page, to spread the word and improve access to community information and opportunities.



this activity requires preparation and implementation in more than one meeting



computer/tablet/smartphone with internet access



Take it further – How could you use the internet to kick start a community project? Some very successful community groups use the internet to connect people looking for a bit of land for growing their own food with unused land around the community. Others use it to advertise items they want to recycle or to enable people to trade skills, for example, someone who can teach Spanish looking for someone who can teach them basic computer skills. How about a newsgroup that collects and shares volunteering opportunities for young people? Survey your community and identify a need that you think can be met by using the internet.

Learn more about community action projects in WAGGGS here:
www.wagggs.org/en/resources/document/view/25247



TIP!

Don't like what someone is saying?
Hit block.

6 online adventure

One of the greatest things about the internet is that it puts opportunities you didn't even know existed right on your screen. What would be your ultimate adventure? Perhaps a trip to a country you've never heard of before, or a powerful challenge to get your pulse racing? Imagine your perfect adventure, then use the internet to put together a virtual scrapbook of your trip with information and media you find online. Share your adventure with your group and display it at home to inspire you.



15 mins



computer/tablet/smartphone with
internet access and printer



Take it further – What if your dream came true and you could actually book your adventure? Research how you could use the internet to plan the perfect itinerary, get insider information and track down the best deals. However, not every deal is as good as it looks so learn to spot holiday scams. Visit some of the internet safety websites listed in the back of the pack for tips on using the internet to plan trips.



20 min



computer/tablet/smartphone
with internet access



7 Block it!

Set up an obstacle course at your meeting place. Blindfold two team members and have them walk from one end of the course to the other. Each has a 'guide' walking with them but the guide can only help with their voice. How easy is it to navigate the course without touching the obstacles?

Discuss: This game is a bit like going online; the blindfolded person is like someone using the internet who can't always see the security risks around them. The guide represents security software that can help the user navigate the web safely. However, security software cannot do everything on its own. The blindfolded person has to cooperate and be careful, using their other senses and not running ahead. When using the internet, users need to be as smart and careful as they can be. That, combined with good security software, will help keep them safe online.

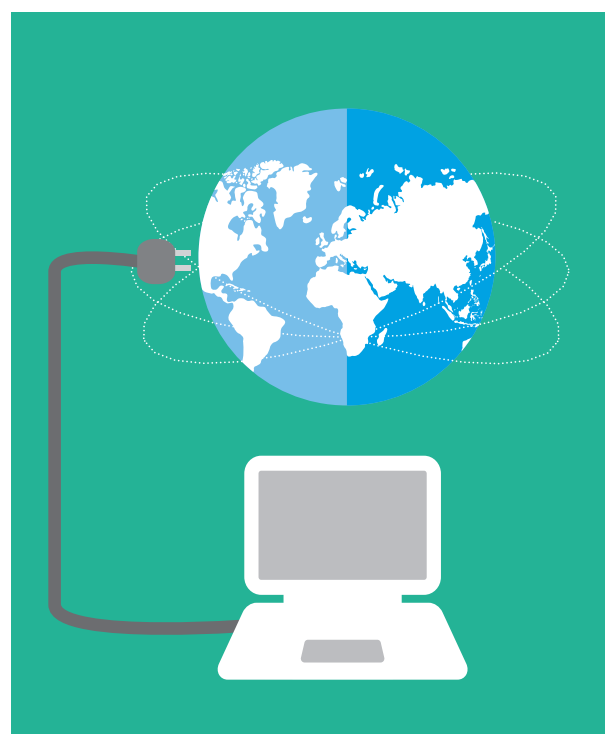


15 mins



objects for obstacles, one scarf or
blindfold for each participant

ALL AGES



*A single Google query uses **1,000** computers in **0.2 seconds** to retrieve an answer*

8 Best of the web

There are so many great websites out there, you can't try them all. Instead, share your knowledge with your friends! In groups, talk about your favourite sites, what they do and why you like them. Create a visual map of the great websites your group recommends and arrange them by use, for example, social networking, listening to music, learning about an outdoor activity or playing games. How do you think this list could help someone looking for new sites or going online for the first time?



20 mins



computer/tablet/smartphone with internet access, paper, pencil, coloured pencils for all participants

ALL AGES

Take it further – Is there anything you know how to do online that someone from an older generation doesn't know how to do? Talk to an adult you trust and find out what they would most like to know how to do online, then teach them how to do it. You can also use the list of interesting websites you created in the above activity as a reference and for examples.



20 min



computer/tablet/smartphone with internet access

+13



Safe searching

The internet is the biggest library you'll ever find, and anyone can contribute to it. However, that means that not everything you'll find online is reliable. Content doesn't have to be written by experts, and people can have lots of different opinions that affect the way they write about something.

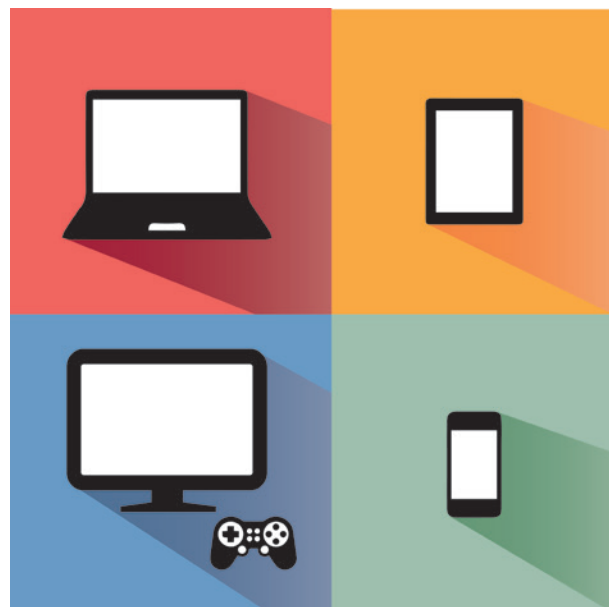
So how can you be sure your searches give you reliable information?

- **Use more than one word to describe what you're looking for.** For example, if you want to know more about the musical culture of Brazil, searching for "Brazil dancing music culture" will give you more specific information than just "Brazil".
- **Stop and think about the words you're using before you hit "search".** Do any of them have other meanings that could bring up unwanted results?
- **Verify your information.** Not everything you find online can be trusted so be a smart researcher and check at least three sites to verify the information and don't forget to look in books or talk to people who might know.
- **Check your search filters, particularly if you're looking for images, to avoid inappropriate material.** Check your search settings and select the highest safety settings.
- **Want to go back to a site you've already visited?** Bookmark your favourite websites or check your history lists to make sure you're revisiting the same page.
- **Check your spelling!** A small typing mistake in your search can bring up results you don't want.

Security software can protect you from fake websites. Download browser tools or use those in your security software to identify imposter sites and keep searches safe. Some may also show site ratings.

TIP!

Is someone acting out of order on an instant messenger, chat room or online game? Use the Print Screen button to take a screen shot of the messages, then open a paint programme, paste the screen shot and save it as evidence.



9 Text treasure hunt

How can you use mobile technology to freshen up a familiar activity? Try organizing a text or email treasure hunt for your group. Explore your local area and think up clues a group could follow to find specific places as well as a question about each place they can only work out once they are at the location. Send the group out with a mobile phone and text them the first clue and question. When they text back the answer, text them the clue and question for the next place. How did using a mobile phone change the experience?



30 mins



computer/tablet/smartphone with internet access per group



Take it further – Try other ways of using mobile technology in activities. Think about incorporating apps from a smartphone and set a challenge where the youth members would need to use at least 5 different apps in their phone such as: Google maps, QR codes (a type of bar code your phone can read), audio recorder, calculator, compass, camera, etc.



30 min



computer/tablet/smartphone with internet access per group



Going mobile

Surfing the web is no longer just about computers. With mobile phones, tablet devices and handheld game consoles, you can now be connected almost anywhere. It's just as important to be smart when using these devices as when you're sitting in front of your home computer. Some basic guidelines:

- Anything sent in an instant message or SMS can be easily forwarded and shared, so think twice before sending anything you wouldn't want someone else to see.
- Most mobile devices can be password protected. Put a password on your phone – it stops your information being accessed if it's lost or stolen, and keeps your friends from using up your allowance!
- There aren't many mobile phone viruses yet, but they are around. Be careful about clicking on an unknown link or replying to an unexpected text. Check that the security software for your brand of mobile phone is up to the task.
- Never give out your mobile phone number to someone you met online but don't know in person.
- Keep an eye on how much you are spending and know your limit.
- Be careful how much time you spend on your phone, especially in the evening before going to sleep. There are studies which warn mobile and tablet users peering at brightly lit screens in the evening as it disrupts the body's natural rhythms and results in poor sleep.

TIP!

Using your mobile when out and about? Be aware that if you're on a call, you're not necessarily paying close attention to your surroundings, so keep the call short, particularly if you're out late.

DISCUSS:

How do you make your blog totally private?

10 School of the future?

Have you thought how technology has affected the way we learn? Sugata Mitra, winner of the TED prize in 2013 introduces a different type of school: a school in the cloud. Watch his inspiring TED talk www.ted.com/talks/sugata_mitra_build_a_school_in_the_cloud where he presents his project and discuss with the rest of the group what you think about it. Would you be interested in a school like that? How different is it from your school? Do you agree with his view?



40 mins



computer/tablet/smartphone with internet access



Take it further – Learn more about Sugata Mitra's project based on a Self-Organised Learning Environment (SOLE) www.theschoolinthecloud.org Share your opinion using your group's social media account and invite your friends to share their opinions too.



20 min



computer/tablet/smartphone with internet access



Blogging

Blogs are an online journal where people share their opinions and feelings, and capture moments from their lives in text, images and videos. You can make your blog private, share it with people you know or make it public. Blogs are great ways to practise your writing skills and be creative, and you can also use them to connect with others who share your interests. Blogs work best if they stick to a particular topic or interest. Instead of describing what you had for breakfast, focus on something you love - the more specific the better! Whatever you blog about, check you blog safely.

Tips to blog safely

- Check your privacy settings before posting. If your blog can be accessed by everyone you know, don't post anything that you wouldn't want everyone you know to see.
- Remove any personal information from your blog or profile that could be used to identify you, such as full names, ages, locations, phone numbers, or the name of your school.
- Learn how to manage comments or block them altogether. Be ready to monitor your blog for inappropriate comments and remove them.
- Remember that once something is posted online, it cannot be taken back. Even if you delete a post, its content could have been copied.
- If anything on your blog site makes you feel uncomfortable, such as others making comments you don't like, speak to an adult you trust.
- Don't start a blog for the sake of it. Wait until you have a clear idea what you want to write about.

Show your blog to a trusted adult and ask them to keep an eye on what is posted there.

In 1 second there are:

8,480 Tweets sent,
1,701 instagram photos uploaded,
1,720 tublr posts,
1, 651 skype calls,
95,156 YouTube videos viewed,
2,367, 473 emails sent



11 Blog about it

Have you ever thought about starting a blog? Blogs are a great way to practice your creative skills, like writing and photography, but it's important to plan in advance what you will blog about and have a clear idea of what information you are happy to appear on your blog and what you want to keep to yourself. The most successful blogs focus on topics people are interested in. What do you know about or want to learn more about? Make a list of blog topics you think you'd enjoy writing about and share them in your group. What would your friends find most interesting to read? Set up a private blog to share with your friends and family, and keep it updated for one term.



this activity requires preparation and implementation in more than one meeting



computer/tablet/smartphone with internet access



TIP!

Remember to log off when you have finished with a webpage.

12 Photo story

Do you like taking photos? Why not use them to tell your own story! Decide what message you want to share, plan it as a series of images, and take photographs that when displayed in a certain order, say what you want to say.



20 mins



camera/tablet/smartphone and printer

Take it further – Upload your story to the internet using a service that gives you privacy control, such as Flickr, Google+ Photos, Instagram or a Facebook group, so you can control who you invite to view your story, then share it with friends and family. Learn about watermarking your photos and how it can prevent others from copying your images, then try it yourself.

Remember that you can share your photos with other Guides and Scouts around the world on www.waggs.org/en/internetsafety!



10 min



computer/tablet/smartphone with internet access



Creating for the Internet

When you upload your content to the internet you are entering into an agreement with the web service you upload it to. Whether it's Facebook or YouTube, a blogging site like Tumblr or a photo site like Flickr, by uploading your content you're agreeing to the "Terms of Service" or "Terms of Use" of that site - the rules of an online service provider that users must obey.

When you create original content, you automatically have content ownership rights. Original content is anything which was 100 per cent created by you – a recording of you singing a song you wrote, for example, not singing a song written by someone else. When using most online services, you keep those content ownership rights. However, there are lots of ways that online services can still use your content without taking your ownership rights – and these will appear in the Terms of Service or Terms of Use.

If you look up the Terms of Use for a service you use, you will probably find a sentence that looks a bit like this:

"By submitting content to our Service, you grant us a worldwide, perpetual, non-exclusive, royalty-free license to use, copy, adapt, modify, publish, display and distribute your content in any media"

That means the service can do anything they want with your content, even though it remains your property. They can share it with others all over the world for as long as they want, change it as they want, publish it in any form, and give it or sell it to other companies to do the same. These terms don't just apply to videos and photos and can also apply to posts and tweets on social media sites. The only way to be sure you're happy with how a web service uses your content is to check their Terms of Use for yourself.

Protect...yourself from online risks

Complete any two activities to earn your badge!

TIP!

Age restrictions online are there to stop you seeing something you really don't want to see. If a page says "18+", log off and tell your parent/carers.



1 Show it off

In a small group, decide on three basic tips you think are important to keep you safe online. Create a dance, song or show that communicates these tips, and perform it for your group.



15 mins

ALL AGES

Think about how you could make your basic tips easy for younger members to understand then perform your piece for a younger age group. Afterwards, talk to them about the message of the piece.



15 mins



Take it further – Record your performance and upload it to the WAGGGS YouTube channel. Remember to check that everyone involved is happy to appear online.



15 min



TIP!

Check the privacy settings of sites where you post information.

DISCUSS:

What should you do if someone in a chat asks you to send them your photo?

2 Perfect password

A good password uses a mixture of letters, numbers and symbols. It should be hard for someone to guess but easy for you to remember. In a small group, take turns choosing a memorable object or a favourite phrase or saying, such as a line from your favourite book or film. Each person then thinks how to turn this phrase into a hard-to-guess but easy-to-remember password with at least eight characters, using a mixture of letters, numbers and symbols. To help, draw a grid with two rows and as many columns as there are different letters in your password. If using a phrase, use the first letter of each word. Write the letters in the top row and a corresponding symbol or number below it.

For example, here the easy-to-guess word "butterfly" becomes "B@++3rf1Y", which is a much better password.

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| B | U | T | T | E | R | F | L | Y |
| B | @ | + | + | 3 | r | f | 1 | Y |

Write a few passwords using this code, then give your passwords to a friend and see if they can decipher them.

Discuss: Can you think of any other ways to make a complicated password easy to remember?



10 mins



paper, pencils enough for all participants

Take it further – Separate the groups into smaller teams, so that every team has a smartphone or a tablet. Ask the groups to search online for apps that are used for password safety and data protection. Allow the teams to research for a while and then present their suggestions.



10 min



computer/tablet/smartphone with internet access



TIP!

Keep your password to yourself, and change it often.

Never click on a pop up, even if it says "close" or "cancel". Always use the red cross to get rid of it.



Good passwords

The key to a good password is finding a balance between something you can remember and something nobody else can guess.

To be sure you've got a good password:

DO...

- Keep your password at least eight characters long.
- Use a mixture of upper and lower case letters, numbers and symbols.
- Log out when you have finished with an online service.

DON'T...

- Only use words you can find in a dictionary.
- Include personal information such as your name or birthday.
- Use something obvious like "12345678", "letmein" or "password".
- Use the same password for every account. Keep unique passwords for really important accounts like your email and social network.
- Enter your password into online forms or send it in emails. If you get an email from a website you use asking for your password, it's probably a phishing attempt and isn't really from that website.
- Share your passwords with your friends. It doesn't mean you don't trust them, it's just good practice.
- Keep your passwords on display. If you need to write them down, keep them somewhere safe and out of sight, such as giving them to your parents. Don't keep them stored on your computer.

DISCUSS:

What are three ways to make a better password?



3 Keep it private

Many places online, such as social networks, cloud storage sites or online games, require you to set up an account and personal profile. Do you know how many accounts you have? As you use the internet over the next week, list all the places online where you have an account. "Greenlight" your accounts by checking that you've chosen privacy settings and created a secure password for each one on your list.



10 mins



computer/tablet/smartphone with internet access, paper, coloured pencils



Take it further – Race against time and try this quiz by Symantec to learn how to spot risky sites:
www.staysecureonline.com/staying-safe-online/quiz/

How many correct answers did you get out of 10? If you got less than 5, try it one more time.



5 min



computer/tablet/smartphone with internet access



DISCUSS:

Who should keep a copy of your passwords?

4 Beat the virus

What is a computer virus? Why do people create viruses? How are they spread? How can you protect your computer against them? Invite an ICT teacher or computer expert to visit your group to answer these questions and to explain how internet security software works to keep you safe. You can also research online - <http://bit.ly/XUTVb> is a good place to start - and present what you learn to your group.



this activity requires preparation and implementation in more than one meeting



computer/tablet/smartphone with internet access

ALL AGES

*Having household internet guidelines reduces the chance of children having a negative online experience by **30 %**.*

TIP!

If you want to forward an email, remember that you can't control who the email will be shared with once you hit "send". Protect your friends' email addresses by using "blind carbon copy", or "bcc". Learn how at <http://bbc.in/iXeSov>.

DISCUSS:

What personal information is safe to share online?

5 Worms and walls

A group member is designated the computer user. Six others join hands and form a circle around him/her. They are the security software that protects the computer. Four members become malware trying to access the computer. When the leader says "Go" the malware try to touch the computer user while the security software try to keep them away. Next, take away three or four of the security software, telling the group that the computer user hasn't been keeping her software updated. Play the game again. Is it easier for the malware to reach the computer user?

Discuss: Why is it important to keep your security software running and up-to-date? What else can you do to protect your computer and the information stored on it?



10 mins

ALL AGES



Malware

Malware is the name given to the tools cybercriminals use that can damage the information on your devices, trick you into taking actions you don't want to take, and steal your private information. Malware has been around for more than 25 years, and today more and more malware is being written to target social networks and mobile phones. To learn more about some common types of malware look up spyware, computer virus, trojan horse and computer worm in the glossary.

How can you protect your computer from malware?

- Check that your security software is switched on and updates automatically.
- Keep a firewall turned on as well as your antivirus software.

Watch out for spam email and suspicious websites. If you don't trust it, don't click it.

TIP!

Always use a nickname online instead of your real name, and don't give out your real name if someone asks.

Setting up your profile on a social network or chat room? Create an avatar instead of using your photo.

6 Avatars

Imagine you're joining a social network. Instead of sharing a photo, draw an avatar of yourself – a cartoon picture that represents you. Pin everyone's avatar up around the meeting place then ask a leader to call out names of group members at random. Everyone should try and guess which picture represents that person by going to stand beside it. Avatars are a great way to express your own identity online without giving away information about yourself to strangers.



15 mins

ALL AGES

Take it further – after everyone introduces their avatar, ask one of your group members to start a story using their avatar, for example: 'One very rainy day Bjork (the avatar), an elf living peacefully in the forest, heard a loud knock on the door of her cabin. She stood up and...' then the next person will continue the story introducing her/his avatar. Let your imagination run free and be as creative as you can with your character to progress the story.



10 min

ALL AGES

7 Free Being Me

Magazines and advertisements often use airbrushing to create a 'perfect looking' image of models and celebrities. Brainstorm with the group different ways that this image editing is used and then watch the 'Dove evolution' video www.youtube.com/watch?v=iYhCn0jf46U.

Discuss: How realistic or unrealistic is the outcome of the airbrushing technique? How does this "perfect looking" image that the media creates affect our self-esteem and body confidence? Want to learn more about self-esteem and body confidence? Why not download WAGGGS' educational resource: www.free-being-me.com



20 mins



computer/tablet/smartphone with internet access, paper, coloured pencils



Take it further – be a media detective!

Work individually or in groups to find and expose an example of the 'perfect looking' image that you have come across in your society's media. Print it out or save it in your computer and write down why you don't agree with it. Then present it to the rest of the group.



10 min



computer/tablet/smartphone with internet access. Optional: printer, paper, pencils



8 Faceless to faceless

How do you know if the person you meet online is who they say they are?

Choose a favourite character from a book or film and create what you think their social network profile would look like and what information it would contain. Create a paper version of this imaginary profile, or act it out - but don't mention the name. Swap profiles and try to guess who your friend has chosen. Do you think you know more about this person now? Can you trust the information you find in an online profile?



15 mins



paper and colour pencils enough for every participant

ALL AGES

Take it further – Imagine your friend was getting to know your imaginary person through a chat room, and that you were worried the person was lying about their identity. What advice would you give your friend? Imagine the questions and opinions your friend might have, then write a letter to them explaining your advice, or write and perform an imaginary dialogue with a friend on this topic. How do you think you could help your friend, and is this different to how her parents might be able to help her?.



15 min



paper and colour pencils for each participant

+13

TIP!

Meeting up with an online friend can be risky. If you really want to meet, speak to an adult and be sure they go with you.

9 It's what you know

Everyone writes on slips of paper two or three facts about an imaginary person and puts them in a container. Divide the group into two teams and place the filled container at a start point and an empty container at an end point. These should be as far apart as possible in a large indoor or outdoor area. Team A gathers at the start point and Team B spreads out over the area. At 'Go', each member of Team A takes one fact and tries to put it in the empty container without being caught. If they are caught, Team B takes the fact. Play continues with all players until the facts are either in the end container or captured by Team B. When the game is over, everybody listens to what Team B has learned about the imaginary person.

Discuss: What if the imaginary person was you, and those facts were information that anybody could see online? How would you feel? What do you think a cyber-criminal could do with this information?



15 mins



paper and colour pencils enough for every participant

ALL AGES

*By the year **2020** it is predicted that over **50 billion** devices will be connected to the internet, equal to seven for every person on the planet.*

10 share the learning

In groups, plan an information evening about internet safety for a group of your peers or younger members of your community, such as a younger Guide and Scout group. Work out what they need to know and plan a set of fun activities that introduce internet safety ideas without using a computer. You can use the activities and games in this pack or create your own.



depends on the chosen activities for the planned event



depends on the chosen activities for the planned event



Cybercrime

Cybercrime is the name given to the actions criminals take online. Cybercrime is fairly common: globally, two-thirds of adults using the internet have experienced cybercrime.

Types of cybercrime include:

- damaging your computer by deleting information or damaging software.
- stealing private information off your computer or home network, such as your email address or bank details.
- persuading you to send money, often using false stories about investment opportunities, winning prizes or someone you know being in trouble overseas and needing money.
- confirming your email address is real so more spam mail can be sent to you.
- using your email account (often without your knowledge) to forward spam in order to find out the email addresses of your friends and family.
- identifying you – with enough personal information cybercriminals can take advantage of you in real life, such as by approaching you at a place they know you visit, or can pretend to be you online.
- deliberately upsetting or frightening someone.

Remember, cybercrime is as illegal as offline crime. If you come across something you don't think can be trusted don't respond – block it and tell an adult you trust.

*Every **60** seconds on Facebook:*

510 comments are posted,
293,000 statuses are updated,
136,000 photos are uploaded.

TIP!

Check with a parent/carer before downloading anything.

Downloads can contain malware that could mess up your computer.

11 Spamcast

In groups, research the main internet security threats – malware, phishing and scam emails. Plan and record a series of short podcasts informing people about these threats and what to do about them. Use different ways to make the topic interesting and entertaining, such as mock interviews, top tips and news stories.



depends on the podcasts



depends on the podcasts



Take it further – Why not create a podcast series that you can upload in SoundCloud, Archive.org, Ourmedia.org, Podomatic or other podcast websites. Make sure that you cross-check that the information you are sharing is correct and up to date.



DISCUSS:

How much information does someone need to be able to find you?

12 Go phish!

Phishing is when an email or website tries to trick you into giving away private information such as account details. Many phishing emails get caught by the spam filter in your email account, but some do slip through, and it's not always easy to spot the difference between a genuine email and a phishing attempt. Go online and play this game: www.onguardonline.gov/media/game-0011-phishing-scams



10 mins



computer/tablet/smartphone with internet access



Take it further – research online for examples of phishing emails as well as correct versions of those emails and print them out – at least 6 different examples. At first, only display the phishing emails somewhere for all the group members to see. Give colour pencils to each group member and ask them to colour the different parts of the email that appear suspicious. Now show the real emails and compare them to check if the comments are correct.



10 min



computer/tablet/smartphone with internet access, printer, colour pencils



Phishing and email scams

Email scams are messages that try to talk you into giving out information or sending money to someone you don't know. They generally tell a tempting or dramatic story and try to get you to react emotionally so you follow their instructions without thinking.

Phishing is the name given to a scam that is trying to steal information from you by pretending to be a message from an organization you trust. Phishing often happens by email, but you can also get phishing phone calls and text messages. The messages may be trying to get you to do something harmful such as opening an attachment that contains a virus, going to a risky website, or giving out personal information.

To protect yourself from scam emails and phishing attempts, look out for:

- Emails from people you don't know or you're not expecting.
- Emails from someone in your address book but written in a way that doesn't sound like your friend, or giving you instructions that seem strange, like "I've found this great offer" or "click here to see the video".
- Messages that aren't addressed personally to you, such as calling you "Dear Customer" instead of using your name.
- Messages that use dramatic language or tell unlikely stories.
- Any email that tells you to enter your password or other personal information, verify your account or click on a link.
- Attachments you weren't expecting, or with strange names and programme file types, such as file names ending with ".exe".

It can be quite hard to spot a phishing attempt, so to be safe try following these basic rules:

- Never click on links in emails. Instead, type the link address directly into your browser.
- If you suspect an email might not be genuine, don't react or reply to it. If it says it comes from a friend, contact them directly by some other means and check if they sent the email.

If in doubt, hit delete!

Respect...your rights and reputation online

Complete any two activities to earn your badge!

1 cyberbully

Why do you think people might be unkind to each other online? How does it happen, and what could you do to stop it? Look at the definition of cyberbullying (p. 39) and ask your leader to show you some advice videos that explore what cyberbullying is like and how to stop it, then complete one of the following two activities:

DISCUSS:

Can a cyberbully be traced?

Is it legal to cyberbully someone?

Would you know what to do if you, or a friend, was being cyberbullied? Using the advice on page 26, create a play to raise awareness about cyberbullying and remind people what to do about it.



duration of this activity varies



computer/tablet/smartphone
with internet access



Take it further – Develop your play into a movie about cyberbullying, using locations in your local community. Hold a movie launch party and share your film with friends and family.



material depends on the type of survey
and reporting you would like to do



material depends on the type of survey
and reporting you would like to do



Conduct a survey about cyberbullying in your school or community group to gather the opinions and experiences of your peers. Turn your findings into a report, for example, a poster showing statistics, that promotes positive online behaviour. Can you get your report published by your school and/or local community, either online, offline or both?

Remember to share your results with WAGGGS at www.wagggs.org/en/internetsafety



depends on the type of survey and
reporting you would like to do



depends on the type of survey and
reporting you would like to do

ALL AGES



cyberbullying

When someone uses technology to deliberately and repeatedly be cruel to someone else, it's called cyberbullying. Often, it's not meant badly – it might just be someone passing around a joke. But if it hurts someone, it's wrong. It can happen to anyone, and leaves people feeling alone and unsafe. It can include:

- excluding people from online conversations.
- tagging images inappropriately.
- sending mean text messages or emails.
- putting unkind images or messages on social networking sites.
- imitating other people online.

Nobody likes to be treated unkindly, whether face to face or online. Cyberbullying can be particularly upsetting because it can happen at any time or place – it reaches its target whenever and wherever they access the internet or their mobile phones. If it takes place in a public space, like a social network, lots of people can be involved, and the person who starts it can feel anonymous – and safe – because it can be very difficult to know where an unkind action started.

What if it happens to me?

- Don't respond. Change your privacy settings and block the person responsible.
- If there is a "report abuse" button, click it.
- Save copies of the emails, texts and conversations.
- Find someone you trust, such as a good friend or family member, and talk to them about it.
- Don't assume nothing can be done. Cyberbullying is a crime in many countries, and a bully can often be prosecuted by law.
- If the person being mean to you goes to your school or is sharing cruel messages with classmates, speak to a teacher you trust for advice. The school may have a policy and tools to help you.

2 Spot the difference

A volunteer leaves the room. The rest of the group chooses a scenario and something that makes the volunteer different from them, for example, the group are scuba divers and the volunteer is a mermaid. The group starts improvising the scenario. The volunteer returns, joins the improvisation and tries to figure out who the group is, and how he or she is different from the group. The volunteer can talk with the group and ask questions. Repeat the game several times with different volunteers and scenarios.

Discuss: How did it feel to be different? Was the group welcoming or unfriendly? How could they have behaved differently? How could this relate to your experiences online?



15 mins



What if it happens to my friend?

If you are aware that someone is being cyberbullied, you can help.

- Don't take part. Forwarding unkind messages or pictures makes you part of the act even if you didn't start it.
- Talk to your friend and make sure they know you support them and that they aren't alone.
- Speak out to a trusted adult and report what is going on.

3 Stop that post!

Place one person at each end of the meeting space. One is the sender and one is the receiver. Give a small object to the sender. This represents a message being posted online. The rest of the group divides into two teams. One team tries to carry the post from one end of the hall to the other by passing it secretly between as many team members as possible. The other team tries to identify who has the post and stop it by touching the person holding the object on the arm. Encourage different strategies such as speed and dodging, subtle and secretive, or distracting the seeker team.

Discuss: Messages can spread very quickly online. What do you think you can do to be sure that your online posts don't have negative consequences?



15 mins



small object,
such as a ping pong ball

ALL AGES

Take it further – Work in pairs and create a list of criteria you need to consider when you post something online. Give each group about 10 minutes to work on their list and then feedback to the rest of the group. Ask someone to keep notes on a piece of paper with all the criteria and then ask the group to vote for the top 5 things they need to consider when posting a message online.



15 min



paper and pencil for each participant

ALL AGES

DISCUSS:

How do you know someone is who they say they are?

4 cyberfriends

Having good friends is important to everybody. How can you be a good friend in your daily life and on the internet?

Discuss: How the way you treat your friends online can affect your friendships in daily life. Think of three simple ways you can be a good friend online then create a picture showing your ideas as a promise you make to your friends. Swap promises in your group and display your friend's promises at home.



10 mins



paper and coloured pencils for each participant



Take it further – Once every day for the next week, make an effort to post a positive message online, to make others feel good about themselves, as part of your regular social networking activities.

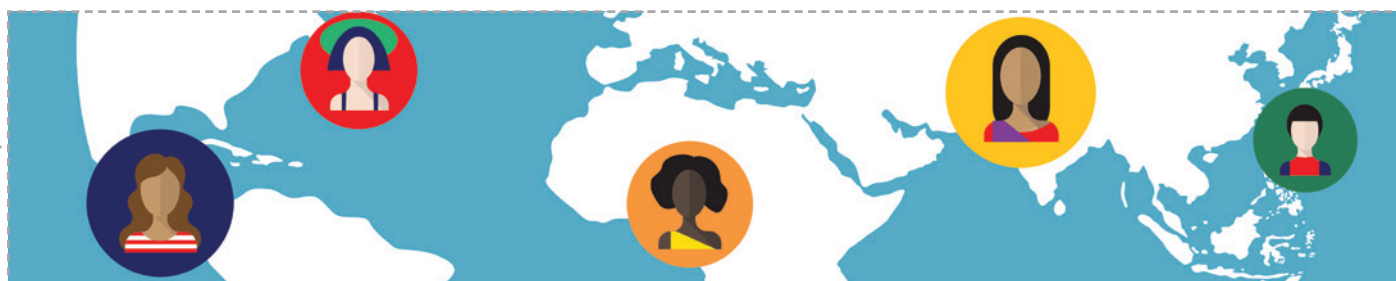


one week



computer/tablet/smartphone
with internet access





5 online anonymous?

Collect news stories about censorship and anonymity online. When is being anonymous online a good thing, and when might it be a bad idea? Do you think it's OK for online content to be censored (hidden from people)? Divide into two teams, one to represent the argument for censorship and the other group against. Allow some time for the groups to discuss and come up with 3 key points for their topic. Then feedback to the rest of group.



20 mins



enough paper and pencils
for each participant

ALL AGES

Take it further – Using the key points from the above activity and with some additional research, plan a debate about censorship or online anonymity, with one side arguing “for” and the other “against”. Research your case and hold the debate, inviting your friends and family to attend.



depends on the type of survey and
reporting you would like to do



depends on the type of survey and
reporting you would like to do

+ 13



Know your tracks

It's easy to think you're anonymous when you're online, but that's not the case. Every time you go online you leave a trail. That's not necessarily a bad thing if the information about you is positive and doesn't reveal any private information. Everything you or anyone else posts about you adds up to your “digital footprint”. Here are some tips to help you understand the mark you're making on the internet.

- Do a vanity search by typing your name into Google and seeing what comes up. If lots of people have the same name as you, try adding words such as the country or city where you live.
- Look at the history section of your website browser to see the websites you have visited in the past.
- Every online device is given a special number to identify it when it is connected to the internet. This is its IP address. If they need to, websites and organizations like the police can use IP addresses to identify who has performed a certain action online.
- Nothing you upload to the web can ever really be deleted. Individuals who want to know more about you can learn a lot by searching for you on the internet – so be careful how much you share!

If you don't like what you find, first see if you can delete any of the content, but remember that even if you delete that embarrassing post or photograph, you can never be sure that it's really been wiped from the internet. Your next step should be to create positive content about yourself online, safe content that doesn't reveal anything personal about you and presents you in a positive light, so you can encourage positive search results that will push you to the top of Google.



DISCUSS:

Can sharing music files online allow others to access your computer?

6 What's the pattern?

A volunteer leaves the room, and the rest of the group sits in a circle and chooses one person to start an action such as clapping hands, tapping their head or patting knees. This person can change the action at any time, and the others should follow. The volunteer is called back, stands in the middle of the circle, and tries to spot the person who is changing the action. They have two guesses. Play this game a few times.

Discuss: How easy is it to spot the person responsible for changing the action? How difficult would it be to spot the person responsible for starting a rumour or sending a message online? Would it be easier to find out where the message came from if not everybody copied the person changing the action or spreading a message?



10 mins



7 Good reputation

Your digital reputation is the online image you present through your online actions. This includes the photos you upload, blog posts you write, emails or texts you send and comments you make in chat rooms, messenger services, forums or websites.

Imagine you're applying for a job or a course. Write down five things you'd like to say about yourself in your application then look at your social network profile and search for your name on the internet. What do you think are the top five things your online profiles say about you? What can you do to be sure that the person offering the job or course sees what you want them to see if they do an internet search for your name?



10 mins



computer/tablet/smartphone with internet access, paper and a pencil for each participant





Digital reputation

Don't be the one with regrets. That joke you texted about your teacher - how would you feel when it suddenly appears on his or her desk? Or that photo of you partying - in five years' time, is that what you want your new boss to see when he searches online for your name? Your digital reputation is what others think of you through how you act online, and unlike something you might say out loud, the internet doesn't forget the things you post. How do you want people to view you? You might not realise it, but you're in control of that. Some tips to keep your digital reputation rosy:

- Check your privacy settings on social networks, to keep strangers from finding information about you.
- Be positive, avoid the negative. Consider what someone you respect might think if they saw your post or uploaded photo.
- If your friend tags you in a photo that portrays you in a negative light, delete the tag and ask them to remove the photo.
- When setting up a social network profile, don't use your full name.
- Keep an eye on your spelling and grammar. Some companies see grammar and spelling mistakes as a sign of immaturity and poor communication skills.
- Remember that posting is permanent, so always think twice before putting something online.
- Monitor your digital reputation by searching online for your name, and ask for anything you don't want online to be removed.
- If you want to get something out of your system, talk to someone face to face.

If you do mess up, act fast to set things straight. Information travels so quickly that if you want to limit the consequences of that nasty post or embarrassing photo, delete it as quickly as you can. Do you owe someone an apology? It looks a lot better if you take responsibility for your mistakes.



8 study smart

Struggling with schoolwork or running late with an assignment? It can be really tempting to find information online about your subject and copy and paste it into your work. The problem is, it's easy for your teacher to spot what you've done and use the internet to trace where you found the text.

Try it out. Working in pairs, one person finds a few paragraphs of text online, copies and pastes them into a word document and emails it to the other person, who tries to track down their source.



10 mins



computer/tablet/smartphone
with internet access



The **first billion** internet users was reached in **2005**.
The **second billion** in **2010**. The **third billion** in **2014**.

TIP!

Set time limits when gaming online and use an alarm.

9 Bridge the gap

When faced with an online problem, you'll often be advised to talk to an adult you trust such as a parent/carer, teacher or community group leader. However, you may not want to do that. In small groups, brainstorm the online problems you have heard of or experienced and decide which problems you should tell an adult about or when an adult's support would help you.



15 mins



paper and pencil

ALL AGES

Take it further – Do you feel comfortable talking to your parent/carers about what you do online? Think of an action you could take that could help you and your parent/carers talk more openly about your internet use, such as giving them a guided tour of your favourite websites, teaching them how to do something online, or coming up with an internet use agreement that you both sign.



15 mins



paper and pencil

ALL AGES

10 online time

How long do you think you spend online each week? Write a list of the main activities you do online such as checking your emails, chatting with friends online, streaming music, playing games or using social networks. Next to each activity, write down how many hours and minutes you think you spend on them each week. For the next week, keep a log of the time you spend on each of the items on your list, and compare them with your estimates. Is there a difference? How long do you think you should spend online each week?



a week



computer/tablet/smartphone with internet access, paper and a pencil



Take it further – With your group, make a blank faced clock with moving hands. With your parent/carers, agree how many hours it is appropriate to spend online each week, and mark this number of hours on the clock. At the beginning of the week, set the clock to "0". Every time you go online, move the hand of your clock forward to show how long you spent online. Is it easy to divide up your time across the week?



5min and then it depends on the research



computer/tablet/smartphone with internet access, paper and pencil



11 Digital footprint

Do you have a sense of how much content you put online? Draw a large footprint outline on a piece of paper and, over the week, every time you post or upload something online, write it down on your footprint – don't put down exactly what you said, just describe it, e.g. "updated my status", "chatted to Raya for half an hour on Messenger", "uploaded 20 photos of my birthday party to Facebook". Share your digital footprints at your meeting place. How long did it take you to fill your footprint? Imagine how many footprints you would fill in a year and how does that make you feel?



10 mins



computer/tablet/smartphone
with internet access, paper and
a pencil

ALL AGES

Take it further – visit the website www.internetlivestats.com and record how many tweets, photos and Facebook posts are uploaded every second in the internet. You can also see the daily CO2 emission from the internet. How does it make you feel to see these numbers changing so fast? Research online about ecology and the internet and try to make an infographic to present your findings to your group.



5min and then it depends on the
research



computer/tablet/smartphone with
internet access

ALL AGES

TIP!

Think before you post – once you click "send", it's out there forever, and you can't control who sees it. Even if you delete it later, someone could have saved it.



On the map

Have you ever wondered how your mobile phone can work out your location on a map?

Location services are really useful. They can tell you where the nearest bus stop or cash point is, help you out when you get lost, and if you're in trouble, the emergency services can use the signal from your mobile device to find you. If your device is lost, you can even use the signal to track it down. But other people can also use location services to find you, and they might not be people you know and trust.

So how does it work? There are three main ways of locating a mobile device (you can find more information on these in the glossary):

- GPS (Global Positioning System) which receives signals from satellites orbiting the earth.
- GSM (Global Systems Mobile) which works in a similar way except it uses signals sent from phone masts instead of satellites.
- Finally, your device can be located through seeing which wireless internet access points, like your home wireless network or Wi-Fi hotspots, your device can communicate with.

If you have an internet phone, it probably uses all three methods combined to pinpoint your location quickly and accurately. Once your device can give your location, there are lots of ways to share it online. However, you can't control who sees this information, and it's a bad idea to let strangers know where you are when you don't know who they are. Think very carefully before using services that use your location, particularly if they make it public.

TIP!

Want to test what you've learned?
Try playing Childnet International's
digital citizen game:
<http://bit.ly/c1Qhzb>

12 Download aware

There is a lot of fantastic digital content online that you can download, such as photos, music and movies, as well apps for your smartphone and tablet but it's important to check you're only using legal sites and not taking anything that's copyrighted without paying for it. Downloading illegal files is called piracy.

In groups, imagine you're a singer who's had his or her music stolen through online piracy. Write a song or rap message to the people who stole your music, explaining how it makes you feel.



20 mins



paper and a pencil

ALL AGES

Take it further – Record your performance and upload it to the WAGGGS YouTube channel. Remember to check that everyone involved is happy to appear online.



20 mins



camera/tablet/smartphone and
internet access

ALL AGES



OK to download?

Streaming and downloading media like movies and music is a big part of online activity, and there are lots of websites that give you easy access to great new material. Unfortunately it's not always legal. It's all about copyright. If you create something original, you own it and have the right to control who can use it, change it or copy it. Artists make their living through royalties, which is the money they are paid every time someone buys a copy of their work - whether it's a CD/DVD, tickets to a concert or movie showing, or a digital version. If you download something illegally, you're taking a copy without the owner's permission.

So you have to make a choice. Where do you get your media, and what will that decision mean for you?

Some thinking points:

- The risk of getting malware on your computer is much higher if you download illegal files.
- It's true that companies that manage artists, such as record labels, often earn a lot more than the artists themselves. However, these are agreements between the artists and the companies, and have nothing to do with our decisions around paying for the content we want, or trying to get it for free.
- Lots of artists are very unhappy to think that what they worked hard to create can be picked up for nothing. When people download pirate copies of an artist's work, they don't consider how the creator feels about it.
- If you use illegal services, you are breaking the law. You might think the chance of getting caught is really small but if you are one of those who gets caught and charged, the consequences can be really big: huge fines, internet bans, a criminal record, even jail time. It could really affect your future.
- Some people say that copying something isn't the same as stealing it because they haven't actually taken it away from someone. But that's like saying that a song or film isn't a product to be bought. If that were true, there wouldn't be new songs or films anymore, because artists, and the industries that surround them, wouldn't be able to make a living.
- Pirate copies are often much lower quality than what you get if you purchase it legally.
- This doesn't mean that you'll have to pay a fortune to get music or watch films. There are some really great ways of getting content legally and they don't all cost money.

Put Yourself First !

You must do this activity to earn your badge!

Now that you have a good idea about how you can make the most of the internet and stay safe at the same time, stop and think about what you have learned. How can you use these ideas in your own life? Imagine you are making a promise to yourself about staying safe online. What would you say?



For example...

"I will stop and think before I post information on the internet."

"I will talk to an adult I trust if something happens online that I'm not happy about."

"I will be careful when opening emails or clicking on links and block anything I think looks unsafe"

Pick your top promises and write them in the box below. Print out the box and share it with your family. Display it near your computer to help you remember what you have learned.

My Internet Safety Promise

I want to stay safe online, take care of my friends and be able to enjoy using the internet.

To make this happen, I promise myself I will try to...

-
-
-
-
-

Signed.....

Date.....

Share!

Share your Surf Smart experience,
the photos you took and videos
you created with Guides and Scouts
from around the world!

There are lots of ways to connect with WAGGGS!



Visit www.waggggs.org



Twitter ([@waggggs_world](https://twitter.com/waggggs_world))



Facebook
(www.facebook.com/waggggs)



Tell us what you think
about the activity pack by
completing an online survey
www.waggggs.org/en/internetsafety



Email your Surf Smart story to
youthlearning@waggggs.org

Notes

Adult internet safety guidelines

These guidelines are aimed at parents, guardians and Guide/ Scout leaders and are intended to help you understand how you can best protect the safety and privacy of young people in your care. Certain points will be legal requirements in some countries but not others, though they can be regarded as best practice even if not legally binding.

Consider the ways you protect children in the real world. You take care to keep them from dangerous physical situations. You monitor where they are, who they are with, what they view, and how they behave. Now apply those same criteria to their internet and digital interactions and think of ways you can minimize harm and ensure that children are protected and safe. As a youth leader you should take care to self-regulate your online activities and prevent your private and public worlds from overlapping.

Email policy

- Create an email system for your group. Select an adult volunteer to be responsible for adding, editing and removing email addresses from the system. Set up mailing lists for parents/carers, members of each age group, and group leaders.
- Use the “blind carbon copy” (bcc) function when emailing groups to protect everyone’s contact details and avoid spam.
- Maintain the list for Guide/ Scout group communication only. Do not forward chain emails to young people. Do not share the list with non-members.
- Avoid direct private communication with children, other than generic group messages.
- If you want to contact anyone under 16 using email or text, you should have written permission from their parent/carer. Copy another adult into any message you send to a member under 18.
- Should a child directly contact you or another adult leader, discuss with other adult volunteers how to best handle this. Depending on the nature of the communication, consider whether the child’s parent/carer should be notified. Your response may vary according to the child’s age: an older Guide/ Scout group member may interact with the group leaders although parents/carers should be informed of this when the child joins the group.
- Consider the content of your message, checking that language and images are appropriate for the age group, and check where the links lead.

Social network policy

- If creating a social network will benefit your group, ensure that the group you create is private.
- Invite group members of an appropriate age, and their parents, to join the group’s social network page or site. Be aware that social networks have different age policies, for example, members under 13 years should not have a Facebook account or use YouTube. Use strict privacy settings to prevent posts and photos from being seen by non-members of your group. When a member leaves, assign an adult volunteer the responsibility of removing the member and parents/carers from the group.
- Create a policy concerning whether or not adults and youth members can accept each other as friends on social networks. Seek parental consent before you accept a child’s online ‘friendship’.
- Define your responsibility and the appropriate actions to take should you observe a youth member posting with bad language, inappropriate images or links to inappropriate content.
- Avoid direct private communication with children, other than generic group messages. Should a child directly contact you or another adult leader, discuss with other adult volunteers how to handle this (see email policy above.)

Photo and video policy

- Create a policy for your group concerning whether or not you will take photos of group activities, and obtain the signed consent of parent/carers to this policy before taking any photos of their child. Include information about whether or not photos are shared with the group members and their parents. While most parents will

like having these keepsake photos and videos, some may object to having their child's photo taken and/or shared for religious, privacy or other reasons. Should parents opt out of photo sharing, be mindful when taking photos and videos that their children not be photographed.

- If you set up photo and video sharing pages online, they should be private and preferably password protected. Obtain consent from anyone depicted in the photos/videos before uploading them.
- Stop and think before sharing any photos or videos of young people online or naming people in images through "tagging". If you do want to share this content, check you have written permission from their parent/carers before doing so.

General security online

- **Secure your own computer and other devices:** Make sure your personal computer and other internet-enabled devices are secured from viruses and malware by using internet security software and be vigilant about scanning for malware. In this way, you can prevent malware from spreading to other group members or gaining unauthorized access to the private member data and financial information stored on your computer or other devices.
- **Use passwords to protect your devices:** Children may ask to borrow or use an adult volunteer's phone, digital camera, tablet or computer. You can prevent them from accessing specific files or programmes on these by using passwords where possible. Be sure there is no objectionable material stored on your device – if there is, you can be sure a child will find it. A password can also prevent a child from purchasing music or apps without your permission.
- **Online banking:** Your group's treasurer should be required to secure their computer with internet security software and to carefully monitor who can access the group bank account, either physically or online. Avoid conducting group financial transactions on public computers or on public wireless networks that could have less secure settings than your personal network. Check the account online at least once a week to verify that transactions are all authorized. Report any strange activity to your bank immediately to minimize losses to the account.
- **Storage of member registrations:** Who retains the private registration forms for your group? If these include names, phone numbers, email and home addresses, health insurance data and database links, they could be valuable to an identity thief. Set a standard for how the physical and digitised copies of these forms are stored and protected.

Protecting group members

- If a young person confides that they plan to meet up with someone they've met online, make sure their parent/carers know this. Recommend that if the parent/carers allow the meeting they should accompany their child and make sure it happens in a public place. While many people make genuine new friends online, there are justified concerns for meeting someone without first being able to establish that they are who they say they are.
- If you find out that children under your supervision are involved in potentially dangerous online activities such as visiting adult or other inappropriate sites, using illegal file-sharing devices, or joining social network groups that promote anti-social behaviour, you must determine your responsibilities to the children, their parent/carers and the community and act accordingly. Discuss the best course of action with other adult leaders. Don't be afraid to 'blow the whistle' and alert the parent/carers of the potential risks and dangers.

Resources

Internet safety

Childnet International online game: www.kidsmart.org.uk

Childnet International website: www.childnet-int.org

EU Kids Online report: www2.lse.ac.uk/media@lse/research/EUKidsOnline/Home.aspx

Facebook privacy information: www.facebook.com/help/privacy

National Cyber Security Alliance: staysafeonline.org/

NetSmartz Workshop: www.netsmartz.org

Own Your Space – eBook for teenagers <http://www.microsoft.com/download/en/details.aspx?id=1522>.

Safety Centre by Google: www.google.co.uk/goodtoknow

Safer Internet Day an initiative of the EU SafeBorders project: www.saferinternetday.org

Think You know: www.thinkuknow.co.uk

Videos showing you how to check some key privacy and safety settings: www.kidsmart.org.uk/skills-school/

Learning and opportunities

WAGGGS website: www.wagggs.org

Network of youth organizations in Europe: www.eurodesk.org.uk

Council of Europe: www.coe.int/t/dg4/youth/default_en.asp

Inspiring talks any various topics: www.ted.com/

Discover how different things work: www.howstuffworks.com

Google cultural institute: www.googleartproject.com

UN agency focused on gender issues: www.unwomen.org

European Youth in action: www.youthforum.org

Coding and programming for children and young people: www.code.org/frozen

Self-Organized Learning Environment: www.theschoolinthecloud.org

BBC website on technology: www.bbc.co.uk/webwise/

Interested in coding? Try <http://studio.code.org/>

Glossary

Airbrushing – to alter (an image, especially a photograph) using photo-editing software or other techniques in order to increase its attractiveness or conceal an unwanted part.

Antivirus – software that is designed to detect and destroy computer viruses.

Avatar – Graphical images used to represent users in online spaces; they may or may not be authentic representations of the people using them.

Bandwidth – the maximum amount of information that can be transmitted along a channel, such as an internet connection.

Blogging – Sharing your opinions and experiences in the form of an online journal where readers may comment on posts.

Cloud storage - a service that allows customers to save data by transferring it over the internet to an offsite storage system maintained by a third party.

Computer virus - a programme that can copy itself and spread from one computer to another, damaging the data stored on the computer and stopping it from working properly.

Computer worm - a type of virus that can travel from computer to computer on its own. It can copy itself and send out hundreds of thousands of copies, for example, to everyone listed in your email address book. Worms can be designed to give cybercriminals access to control your computer remotely, but more commonly they just use up the system memory or network bandwidth, crashing computers and internet servers.

Cyberbullying - the use of information and communication technologies to support deliberate, repeated and hostile behaviour by an individual or group that is intended to harm others.

Cybercrime - any crime that involves a computer and a network.

Digital footprint – the sum of the information trail people leave online.

Digital reputation – what people think of you based on the information visible about you online.

Digital watermark - a pattern inserted into a digital image, audio or video file containing the file's copyright information such as author and rights.

Downloading – transferring a file or programme from a remote system to a local computer or mobile device.

Facebook – the largest social network on the internet. It enables users to create personal profiles and make connections with their friends.

Geo data - digital data that represent a geographical location.

- **GPS** (Global Positioning System) – a navigational system using satellites and computers to calculate the location of a receiver device. Many mobile phones contain GPS receivers. If your phone has a GPS receiver, it can receive signals from satellites orbiting the earth. The satellites send out signals and the GPS uses the distance between the satellites and the receiver (your phone) to calculate where you are.
- **GSM** (Global System for Mobiles) – a standard for mobile communications used by most mobile phone services in the world. It can also be used to identify the location of a mobile device in relation to the mobile phone masts transmitting to that device.

Internet piracy – illegally uploading or downloading copyrighted material over the internet.

Location services – a service that provides the location of a device in the offline world, whether moving or fixed.

Malware – software intended to damage or disable computers and computer systems. Malware includes spyware, viruses, trojan horses and computer worms.

Phishing – trying to acquire personal information, such as user names, passwords and credit card details, by sending a message, either online or over the phone, that pretends to be from a legitimate organization.

Podcast – a series of digital media files, either audio or video, which are released in episodes and downloaded or listened to online.

QR code – a mobile barcode readable by mobile devices, with a camera that directs the user to a website when scanned.

SKYPE – a popular computer program that enables users to set up profiles, make free phone calls, chat and video chat through their computer or mobile device from any point around the world.

Security software – software that protects a computer from a range of threats.


Spyware - a type of malicious software that installs itself on your computer and collects information without your knowledge. It can be hard to find out if spyware is installed on your computer, so it's important to have good security software to protect against it.

Streaming – a way of sending data over a computer network as a steady continuous stream, allowing content to be played back while the rest of the data is being received.

Twitter – a social networking service that enables its users to send and read other users' messages, or tweets, of up to 140 characters in length.

Tagging – identifying someone appearing in a photo or video online by attaching a virtual name label, or "tag".

Trojan horse - a bit like a virus except it is designed to pretend it will do something you want it to do, then secretly take an unwanted action such as copying itself, giving someone access to your computer or stealing information. An example might be a free game or screensaver. You download the file without realising it has a hidden piece of malware inside.



This project has been made possible in part by a grant from the Symantec Foundation, a corporate advised fund of Silicon Valley Community Foundation.

Symantec was founded in 1982 by visionary computer scientists and the company has evolved to become one of the world's largest software companies. They provide security, storage and systems management solutions to customers – from consumers and small businesses to the largest global organizations. Their Worldwide Headquarters is in California, USA.

The Silicon Valley Community Foundation provides visionary community leadership by identifying emerging challenges and addressing those challenges through their grantmaking programs and research. They are also based in California, USA.



