# Be Internet Legends.

## Online safety activities for the whole family

**The Be Internet Legends programme is designed to teach your child the skills they need to stay safe and have a positive time online.**

**The fun family activities in this booklet are based around the Internet Legends code:**

| | |
|---|---|
| **Think Before you Share** | Knowing what's OK to share on the internet and what's not |
| **Check it's For Real** | Spotting the clues for what's real, fake, misleading or a scam online |
| **Protect Your Stuff** | Learning how to keep information secure online and create strong passwords |
| **Respect Each Other** | Understanding what it means to be kind online and respect other people's privacy |
| **When in Doubt, Discuss** | Asking for help from a parent or trusted adult with tricky situations online |

**Each activity has a Quick Guide to support you and your family with important conversations that may arise around each topic. You can also refer to the library at the end of the booklet for useful definitions.**

**Your involvement at home with these activities can really help your child to develop the necessary skills and reinforce the key messages to help them become safer and more confident when exploring the online world.**

Google | parentzone
The experts in digital family life

# Think Before you Share: Family Activity

Children love sharing things online, from pics of their cat to a funny video they want all their friends to see. The trouble is, younger children sometimes don't understand that what they post online can still be seen by someone far into the future, or that some things are best kept private.

**This activity will help you to guide your child through what's OK to share and what's not.**

## 'Thumbs up, thumbs down, thumbs middle'

Read each scenario out loud. Ask each family member to give a thumbs up if they think it is OK to share. A thumbs down if it is not OK to share. A thumbs middle if it depends. Each time, ask one person to explain their choice to the rest of the family.

1. Sharing a picture on social media of your best friend pulling a silly face.
2. Sharing a video because you think it is funny, but it turns out people find the joke mean and someone gets upset.
3. A stranger in an online gaming chat forum asks for your mobile phone number and home address.
4. Your best friend is coming over for a sleepover but has forgotten your home address, so they message you and ask for it.
5. You have accidentally shared too much information that was personal with a stranger and now you are worried about it. Should you tell someone?
6. Sharing a funny cat video in a friends' chat group.
7. Posting a photo of yourself online in school uniform with the school logo and name showing.
8. Posting your home address in a messaging group with people that you've never met in person.

## Quick guide

Scenario 1: Children sometimes don't realise that what they find amusing might be embarrassing or even upsetting for their friend. Remind them to always check before sharing a photo/video of others.

Scenario 2: Remind your child that some things might upset another child, especially if that child is younger than them. Encourage them to think about the contents of a video and whether sharing it could offend or upset others.

Scenario 3: It is possible to disable the chat function on online games. Check your child knows that it is easy to block and report people who are harassing them or sending inappropriate messages.

Scenario 4: In this scenario they already know the person and have arranged a sleepover. Friends will need to know the address. Remind your child about safe ways to share personal information. For example, they could ask you to call their friend's parents.

Scenario 5: Remind your child to come to you or another trusted adult if anything goes wrong so you can act quickly. You can help them to block, delete and report other users.

Scenario 6: Talk to your child about things that are OK to share, e.g a funny, non-offensive video of a cat sent to friends. Encouraging good behaviour online is really important. Using technology positively is one of the things that can keep children safer.

Scenario 7: A school logo could reveal where your child goes to school. It is best to ensure the logo and school name cannot be seen before sharing this kind of photo. This is a good opportunity to talk to your child about accidental sharing.

Scenario 8: Remind your child that there are better ways to share your home address if someone really needs it. See Scenario 4.

Now play the **Interland** game together. Visit **Mindful Mountain** where information travels at the speed of light and there's an Oversharer among the Internauts you know...

Open a web browser on your desktop or mobile device (e.g., tablet), and visit **g.co/MindfulMountain**

# Check it's For Real: Family Activity

Not everything your child comes across online is true or reliable. The tricky part is working out the difference. Learning how to spot the clues for what's real and what's fake, misleading or a scam online will help your child navigate what they see and read online with confidence.

**This activity will help your child spot key clues so they can work out if what they come across online is reliable.**

## Search , Check , Score

### Search

1. Sit down together with a tablet or other device and go to your favourite search engine home page.
2. Check if the safe search feature is turned on.
3. Pick a topic your child knows/cares a lot about (e.g. football, wildlife, favourite actor) and type it in the search box.
4. Click on a variety of results, at the top and several pages down.
5. Look at the points on the below checklist and see if you can spot any clues.

### Check

Does the website have an About page?
Is it clear who the author of the page is? If so, is it someone well-known?
Is it the site of a sponsor or fan (and so maybe mostly positive)?
If the information is negative, can you find out more about the site or source of the criticism?
Is it just one person's opinion/blog or does it seem to be balanced?
If it's a news site, is it a well-known one you feel you can trust? If not you might want to do a search on it to see if people feel it tries to present information in a balanced way.

### Score

**Give each website a rating out of 3**

- 3 = tip-top reliable
- 2 = best to double check with an adult
- 1 = I definitely wouldn't rely on this site for information

### Quick guide

Explore the search results with your child and discuss the 'Check' questions to see what clues you can spot. Encourage your child to tell you about websites they would trust. Can they tell you the signs of a reliable website? E.g. Secure websites start with: https:// Check the URL (web address)
Talk to them about bias – see if they can think about the author and what their motives might be. See if they can spot the spelling and grammar mistakes that may indicate an unreliable website.

Now play the **Interland** game together. Visit **Reality River** where things are not always as they seem. Use your best judgment to decide what is fact and what is fiction.

Open a web browser on your desktop or mobile device (e.g., tablet), and visit **g.co/RealityRiver**

# Protect Your Stuff: Family Activity

We know that some things need to be kept private. This is something that can be hard for younger children to understand. They may think it is OK to share passwords with their best friends and they probably won't know that some people online try to cause others harm and steal their information.

**This activity will help your child understand how to keep some information private and secure online.**

## 'Strong password' recipe

Start with a quick chat. Ask your child if they think password123 is a 'strong' (secure) password. Discuss why it is important to have a password that you can remember but that nobody else can guess.

Together, write your own recipe for a strong password, including all the 'ingredients' needed to build a secure password for online accounts and instructions for how to create the password.

E.g. Ingredients:

3 capital letters

4 or more lower case letters

2 symbols

1 number

## Quick guide

Here are some quick tips to guide your family discussion:

Try to create a different password for each online account so they are not all the same.

Do not share passwords with anyone, even your best friend.

A weak password is one that is easy to guess like your pets name.

Include a mix of capital letters and lowercase.

Avoid using your pet's name, date of birth and other obvious information that may make it easy for others to guess the password.

Include numbers and symbols to make it harder to guess or to 'hack' (a hacker is someone who tries to get access to someone's information without permission).

Use a short sentence instead of one word so it is hard for others to guess but easy for you to remember.

Now play the **Interland** game together. Visit the **Tower of Treasure** where you need to outrun the hacker and build a fortress with strong passwords to protect your stuff.

Open a web browser on your desktop or mobile device (e.g., tablet), and visit **g.co/TowerOfTreasure**

# Respect Each Other: Family Activity

Younger children often don't realise that some messages can be easily misunderstood online or that they can, and should, do something if they witness unkind acts. Sometimes what is meant as a harmless joke shared in public can end up upsetting and embarrassing others, even their friends.

**This activity will help your child develop a better understanding of what it means to be respectful to others online.**

## The 'what would you do?' game

Read the scenarios and then ask each member of the family to say what they would do in each situation.

**A friend is upset because someone is sending them nasty messages online.**

**You have also noticed that people are leaving cruel comments on the photos they post.**

**You are playing an online game and in the chat forum someone is posting nasty jokes and messages that you don't find funny and are upsetting to read.**

**A friend sends you a video of classmates being bullied that they find funny but you find it upsetting.**

**You comment on a friend's haircut in a message saying you think they look different. You meant it in a nice way but they seem upset.**

## Family chat:

Why is it important to be kind to others, both online and offline?

## Quick guide

Each family member will come up with their own answers and have their opinions for each scenario. This is not a bad thing and it is good to encourage a family discussion.

**Scenarios 1 & 3:** Even if something bad is happening to someone else, your child can be an upstander: someone who recognises when something is wrong and acts to make it right. When we stand up for what is right, and do our best to help support and protect someone who is being hurt, we are being socially responsible.

**Scenario 2:** Even if you're not a tech expert, you can help them solve their problems. Flag up that your child should come to you, or another trusted adult, if they are worried about anything.

**Scenario 4:** Discuss how it is easy to misunderstand written messages that are not said out loud, face-to-face. You could come up with some more examples together.

Now play the **Interland** game together. Visit **Kind Kingdom** where you need to stop the spread of negativity everywhere and help restore the peaceful nature of Interland.

Open a web browser on your desktop or mobile device (e.g., tablet), and visit **g.co/KindKingdom**

# Library

**From Phishers to Hackers, it can be hard to keep up with the digital world's jargon. Here are some definitions to help you out.**

## Think before you share...

| | |
|---|---|
| **Digital footprint** | Your digital footprint is everything on the internet that makes you, you. This could include photos, audio, videos, texts, blog posts and messages that you write on friends' pages. |
| **Personal boundaries** | Rules that you make to let others know the safe and acceptable ways for them to behave towards you. |
| **Personal information** | Information about a specific person. Your personal information can be public or private to varying degrees, depending on how sensitive it is. |
| **Settings** | The area in any digital service, app, website, etc. where you can define or adjust what you share and how your account is handled. |

## Check it's For Real...

| | |
|---|---|
| **Encrypted** | When information or data is converted into a code. |
| **Firewall** | A program that shields your computer from most scams and tricks. |
| **Malware** | A term used to refer to a variety of forms of hostile or intrusive software, including computer viruses and other malicious programs. |
| **Phishing** | A phishing attack happens when someone tries to trick you into sharing personal information online. Phishing is usually done through email, ads, or sites that look similar to sites you already use. |
| **Scam** | A dishonest attempt to make money or gain something else of value by tricking people. |
| **Spear phishing** | A phishing scam where an attacker targets you more precisely by using pieces of your own personal information. |

## Protect your stuff...

| | |
|---|---|
| **Hacker** | A person who uses a computer to gain access to private information without permission. |
| **Privacy** | Protecting your personal information and that of others. |
| **Security** | Using good habits for securing hardware and software. |
| **Scammer** | Someone who cheats or tricks someone else into giving away their private information or even money. |
| **Two-step verification** | A security process where logging in to a service requires two steps. For example, you may have to enter your password and enter a code that was sent to your mobile phone. |

## Respect Each Other...

| | |
|---|---|
| **Block** | To help prevent an individual from accessing your profile, sending you messages, etc |
| **Bystander** | Someone who has the power to intervene or report bad behaviour, but doesn't do anything to stop it. |
| **Harassment** | To create an unpleasant or hostile situation with uninvited and unwelcome verbal or physical conduct. |
| **Upstander** | Someone who intervenes to stop and/or report inappropriate behaviour. |