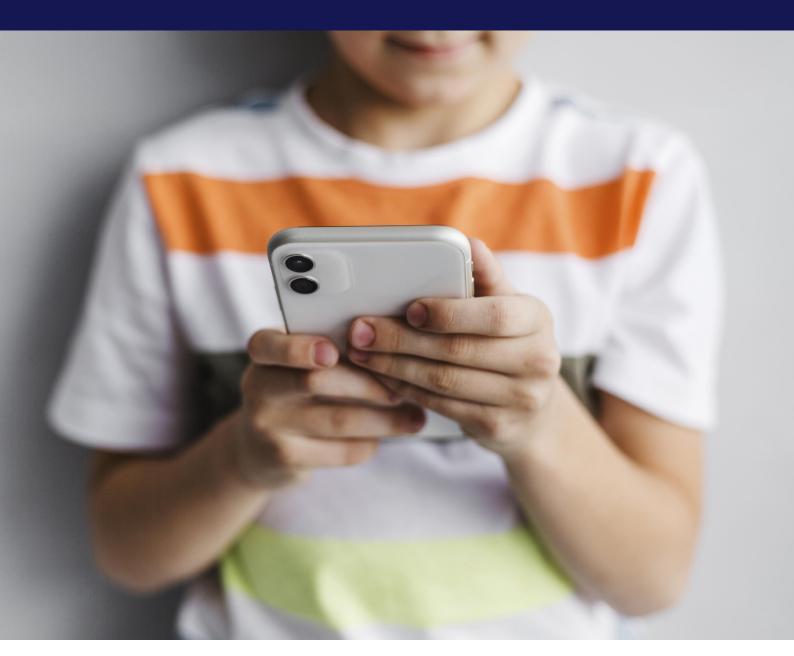


Parent's Guide for the Responsible and Secure Use of Mobile Phones

















## Contents

Introduction	. 2
Background	. 2
The mobile phone: what should you know?	. 3
Back to basics – how a mobile phone works	. 3
Gaming	. 4
Premium rate services	. 5
Social Media	. 6
How you can help keep your child safe	. 6
Top Tips for Parents	. 7
Other useful contacts online	. 7
Glossary	. 8
Code of Practice	7

### Introduction

This booklet has been produced by the mobile operators - eir, Tesco Mobile, Three Ireland,
Virgin Media Ireland and Vodafone Ireland - under the auspices of Telecommunications Industry
Ireland, the Ibec industry representative group. It is designed to provide clear and comprehensive information to parents about how mobile phones work, and what modern handsets are capable of beyond talk and text (e.g. the internet, photography, live streaming content). For the purposes of this document, the person caring for a child i.e. a parent or legal guardian, will be referred to as 'parent'.

It offers parents advice for dealing with any negative experiences that children may encounter with their mobile phone, e.g. cyberbullying, and where to report inappropriate communications as well as providing information on Ireland's official online safety hub 'Be Safe Online', which is a one-stop-shop for online safety resources. It also explains the safety options available to parents, including blocking Premium Rate SMS (see Glossary), and filtering technologies and contains contact details of the main support agencies, regulatory authorities and other useful resources.

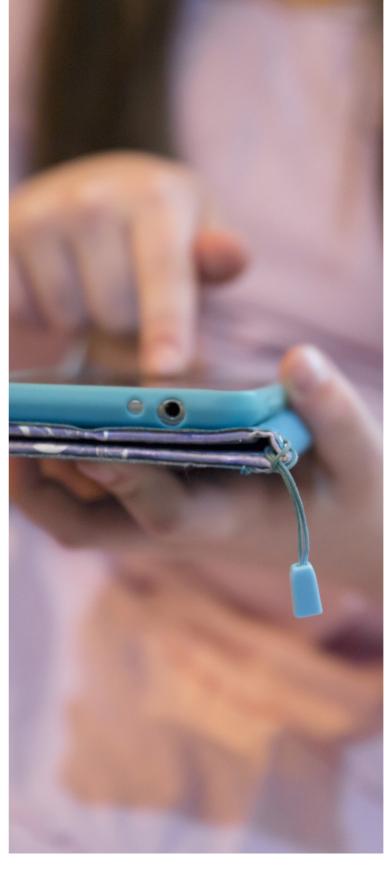
If there are any terms in this booklet which you are not familiar with, please refer to our Glossary at the end of this document.

### Background

Over the last decade, there has been a huge growth in the use of mobile phones – with over a billion users worldwide. For many people, using a mobile phone is a routine part of daily life; it is easy to forget what a sophisticated and powerful piece of technology it is. A person who carries a mobile phone can be contacted almost anywhere and at any time through calls, SMS and through various on-line social media communications services.

Many of us use mobile phones both at work and at home, especially children. CyberSafeKids' annual report from 2019 shows that 93% of 8 – 12 year olds own a smart device, with 44% of this cohort owning a smartphone. Smartphone ownership rises with age, with 20% of 8-year olds and 24% of 9-year olds owning one, compared to 73% of 12-year olds. Used wisely and at the "right" age (which depends on the child's maturity levels and willingness of parents to oversee and engage with their online activity), a mobile phone can benefit children. It can be a fun way for them to stay in touch with friends after school, for example. It can also benefit parents, who can check that their children are safe when outside the home. With the advent of smartphones, mobiles are now packed with all sorts of services. including apps, video streaming, gaming and much more. All of this may seem a bit bewildering to many parents - especially when children are at ease with new technologies having grown up with them.

Parents will naturally be concerned about who their children are talking to, and how they are using their mobile phones. Therefore, it is important for parents to understand how the technology works so that they can make informed decisions, with their child, as to what is appropriate and safe for their use, as well as



how to use their mobile phone responsibly. If parents are more informed, they can prepare their children for their online experiences, and empower them to deal with risks appropriately and ultimately, be safer online. With increased knowledge, they can also encourage their children to use mobile phones in a way that is safe, respects other people, and allows everyone to enjoy the technology's benefits.

# The mobile phone: What should you know?

#### What's Changed...

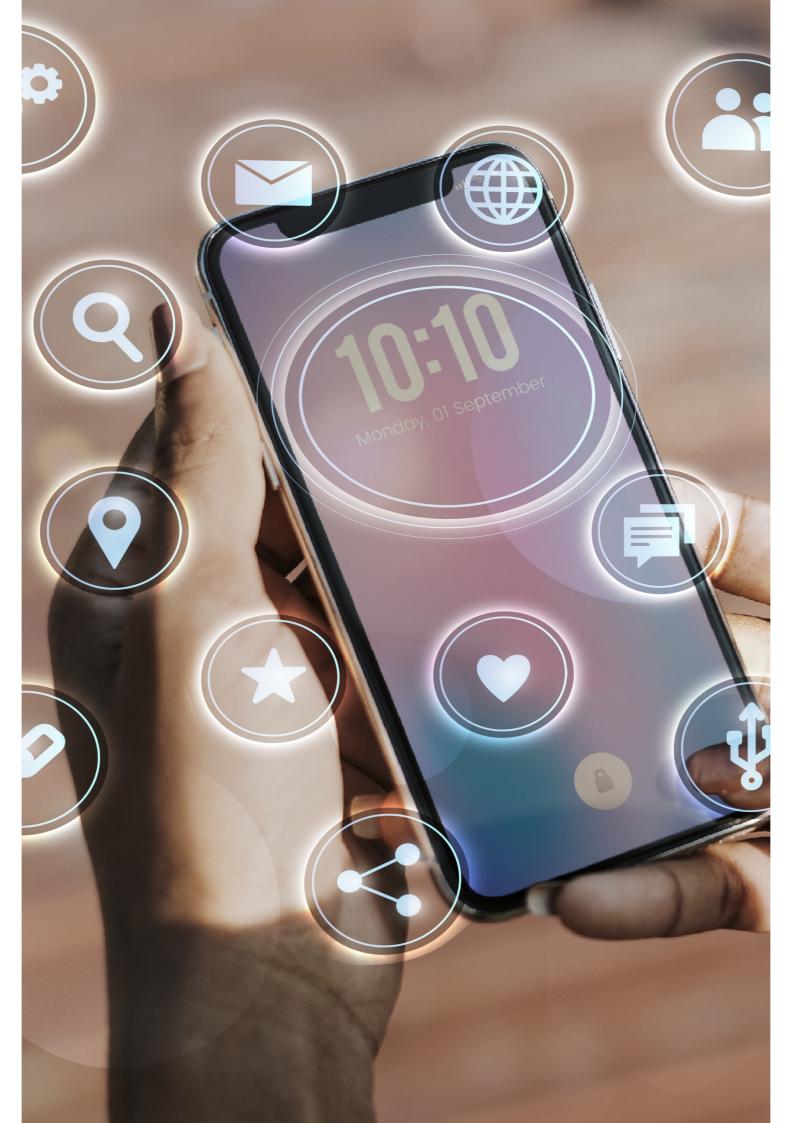
The ways in which children can connect and communicate with each other is constantly evolving. Children don't have to call each other's homes anymore; they can contact their friends directly, wherever they are. There are different ways to communicate too, i.e. talk, text, email, and social media, with social media applications being the most popular. Children can play music, videos, games or browse the internet using their mobile phones. They are powerful devices providing instant access to the online world with a click of a button, which is exactly why we want to provide you with information that will help you ensure your child has a positive and safe experience.

#### What are the Positives?

It is not surprising that mobile phones are so popular among children. Parents too can see the benefits from allowing their children to use mobile phones. Organising family life can be more flexible, for example, arranging times to collect children after sports practice or drama class. A mobile phone can also be used for security, and to check on children's location and safety when they are outside the home. They are also a great tool to connect with friends and the wider family, and of course, are a great source of fun and creativity.

#### What to look out for...

However, children's use of mobile phones has also raised a number of serious considerations for parents. Among these is age. Mobile phones started to become widely available in Ireland in the mid-1990s. Many of today's parents would have purchased their first mobile phone as an adult when they were mature enough to use the technology safely and responsibly. A mobile phone is a powerful communications tool, children cannot be expected to use a mobile phone as cautiously as an adult. This is why it is essential that children are supported and monitored when using mobile devices. They must be as fully prepared as possible through regular conversations, check-ins and the application of appropriate rules and boundaries.



## Back to basics – how a mobile phone works

#### The SIM card

All mobile phones have two major components: the SIM card and the handset.

To send and receive calls or texts (using the service providers network /service), a mobile phone needs a SIM card whereas a sim card is not needed for calls and texts sent using an internet connection / WIFI (this is called Over the Top (OTT) services).

#### **Location settings**

Most smartphones/devices have Global Positioning System (GPS), and therefore they also have location settings that can be enabled or disabled on both the device itself and for an individual app. We would recommend ensuring that location is always set to 'off' for most apps in order to protect a child's location from being shared either deliberately or inadvertently. This is especially important for the camera. With location settings on, any photo or video is created with location and time information stored within the file: this is called 'geotagging'. This information can be easily extracted by anyone who knows how to do it, and if content is being posted in real time, then you are potentially giving away your physical location to strangers.

#### Ways to Pay

Most Irish mobile operators offer two ways to pay for services:

Prepay/ Pay As You Go Bill Pay / Contract

## Gaming

Mobile phones can be used to play video games. Some games allow only a single player. Other games allow two or more players (multiplayer games). Your child's mobile phone may have come with games already loaded on it. Most games can be downloaded or are played online.

Parents should be aware that downloading games or playing them online can be expensive; There is also a risk that they could end up playing games with strangers online. Also, some games – those with violent or sexual content, in particular – are aimed at a mature audience. Many games also have in-game purchases such as loot boxes, and without establishing spending limits in advance, children can quickly run up very large bills within games or apps. It is important that parents set up an e-mail address specifically for their child, specifying their age. This will help prevent children having access to games with inappropriate content.

For more information, check out Webwise's very practical guide for parents called 'Play it Safe – An Introductory Guide to Online Gaming for Parents'<sup>2</sup> which provides helpful tips for parents to ensure a safe online gaming experience for your child. The CommonSenseMedia and PEGI websites will tell you everything you need to know about age limits and content you can expect to encounter in any game available.

#### **Top Tips**

- Ensure that you set up Parental
  Controls around your child's
  device when setting the device
  up initially. The Google Play
  Store and Apple App store both
  have settings that allow parents
  to control what applications
  are being downloaded, how
  much screen time needs to be
  adhered to, setting pass codes
  for all purchases etc. This will
  give you much more control
  regarding what your child is
  downloading on to the device.
  How To: (Google Play) (Apple)
- Where possible, have your children gaming where you can see them – the living room or kitchen for example, so you can keep an eye on what they are doing – especially when they are young
- Check out any game that your child wishes to play first so you are happy that it is appropriate for your child, and be familiar with the different features that each game offers – e.g. chatrooms, private messaging etc. Keep yourself up to date by playing with them from time to time

- Set the ground rules around use: where, when and for how long?
- Keep an eye on who they are chatting to in multiplayer games
- Be aware of in-app spending or disable it so that they must ask if they want to spend money. It is possible to spend a significant amount of money on items such as skins, power ups, virtual currencies, and loot boxes/card packs in games that they play.
- Be aware of loot boxes, which are psychologically akin to gambling but feature in games/ apps that are marketed at children.
- ComReg's website provides
   clear information on what
   Premium Rate Services ("PRS")
   are, how to recognise them, the
   types of charges associated
   with PRS, and details solutions
   to common problems that may
   arise with these services. For
   advice on how to stop a PRS
   or bar PRS entirely, see the Top
   Tips for Parents Section, of this
   guide.

## Premium Rate Services

Premium Rate Services ('PRS') are goods and services that you can buy using your phone credit or bill to pay for them. ComReg is the Irish premium rate services regulator and is responsible for making sure that providers of age-restricted services have the correct age-verification systems in place. Parents can contact ComReg if they are concerned that their children have received content from an age restricted service. (Contact details are at the back of this booklet.)

#### Communicating today

Children can access the internet using multiple devices including a mobile phone, TV, or gaming console, to highlight a few. Online, they can look up information for homework, use streaming services, and chat to friends on instant messaging or social media platforms. Children are now generally accessing the internet through their mobile phones. The same safety rules that parents apply to their children's use of the internet on a PC, should apply to their use of the mobile internet. Parents should encourage their children to tell them or another trusted adult about anything they have seen or heard online that has made them feel uncomfortable or scared. It is important to monitor children's' browsing history regularly in an open and trusting manner.

#### **Social Media**

Social Media platforms have become extremely popular with children. They create a profile, to describe who they are and what they are interested in. They then communicate with friends and/or follow other people online who share their interests and hobbies. Some popular social media platforms include Facebook, Twitter, WhatsApp, Instagram and TikTok.



#### **Top Tips**

- If your child has a profile(s) on social media, they will likely access it on their mobile phone. Ensure they know why it is important to only post or share information with people they know in the real world. It is important to talk with your child to find out about which websites and social media platforms they visit to make sure they are visiting sites appropriate for their age. Also, you should check if these social networking websites / platforms have parental controls available and what privacy policies are in place.
- Be aware of minimum age restrictions for any social media or instant messaging site that your child wants to access and check it out yourself first to make sure it is appropriate for your child. Common Sense Media is a great resource in this regard.<sup>3</sup>
- Agree ground rules around use
- All accounts are set to 'public' by default so it is important to encourage your child to set their account to 'private'
- Encourage children to keep their friends list to just people they know well offline. <sup>4</sup>
   CyberSafeKids found that almost a third of 8 – 12 year olds on social media and

instant messaging apps had friends and followers that they did not know offline.

• Keep an eye on what they are posting and who they are

sharing it with!

- Ensure location services are set to off within the apps they are using as some of these will be set to 'on' by default. Some features also require location to be on in order to send but this should always be switched to 'off' immediately after use.
- Most importantly, have regular conversations about what they are seeing and doing online and encourage them to come to you or another trusted adult if they come across anything that makes them feel uncomfortable or upset.

Webwise provides useful 'Advice for Parents on the use of Social Networking Websites' and CyberSafeKids is another important resource which provides helpful information on online safety for families, including webinars for children and parents.

 Young people often take photographs and videos of themselves and each other on their mobile phones, but they should be very careful with how they share these images. Embarrassing or inappropriate photos/videos could easily be passed between phones and put online. Once sent or

- put online, control over the images is essentially lost and they could end up in the hands of strangers. Photographs or videos could also be used to fuel bullying or harassment. In some cases, such harassment is a criminal offence<sup>7</sup> and we need to ensure our children are aware of this and of the consequences.
- Talk to your children about the risks associated with posting information online – they need to think twice before sharing content – they need to consider would they share this information in the real world with their teachers and friends – would they post this or share this on the school billboard?
- BE SAFE ONLINE<sup>8</sup> is Ireland's official Online Safety Hub – it is the government's campaign to highlight ways to help users stay safe online. The hub provides access to a wide range of online safety resources, to support online safety for all.

https://www.commonsensemedia.org/

https://www.cybersafekids.ie/wp-content/uploads/2021/02/csi\_annual\_report\_2019.pdf. p.29

<sup>5</sup> https://www.webwise.ie/parents/advice-for-parents-on-the-use-of-social-networking-websites-2/

<sup>6</sup> https://www.cybersafekids.ie/

http://www.irishstatutebook.ie/eli/2020/act/32/enacted/en/print - known as Coco's Law

<sup>8</sup> https://www.gov.ie/en/campaigns/be-safe-online

## Cyberbullying and malicious communications

Bullying, in any form, is upsetting for a child.

Unfortunately, new communications technologies have opened up new ways for people to be bullied.

Before the internet, most bullying among children took place in person. By means of a mobile phone, bullying can reach a child at home or almost anywhere, and at any time. On a mobile phone a bully can reach and harass a child directly, wherever they are. Sometimes bullying on a mobile phone is anonymous, if the abusive calls or messages come from a number or profile a child does not recognise. This kind of behaviour can also continue unchecked online, even if the target removes themselves from the situation.

Such bullying is called cyberbullying. On a mobile phone it can involve abusive calls, texts, images or videos or deliberate exclusion from online groups or activities. If you are aware that your child is being bullied, or are concerned that they may be, you should talk to them openly and with sensitivity. Bullying on a mobile phone often, though not always, signals that the child is being bullied face-to-face as well. Parents should take the steps they consider most appropriate if they discover their child is being bullied. All Irish mobile operators have policies which condemn bullying and malicious communications on mobile phones.

Some children hide that they are being cyberbullied because they fear their parents will take away their internet access or mobile phone. In such situations, parents can find it difficult to detect that their child is being bullied because the internet and mobile phone are direct and private ways of communicating. There are some common signs to watch out for with your children. If your child has been a keen user of their mobile phone but suddenly stops using it, or keeps it switched off most of the time, it could be a sign of bullying. Also, if your child suddenly tries to change their number or claims their mobile phone has been lost – and wants a new number for their new handset – it could also be a sign that something is wrong. Other signs include being secretive around the device (e.g. quickly closing or changing screen if others are around, seeming sad or distracted after being on their device, being more withdrawn than usual).

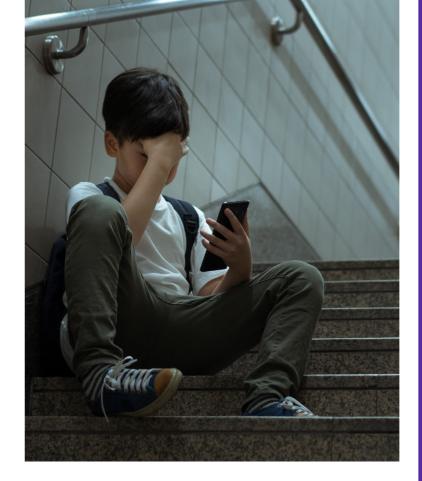
Remember also that parents need to act responsibly if they discover that their child is bullying someone else. Some parents register their child's mobile phone in their own name. If you have done this, and threatening or abusive communications are sent from that mobile phone, you may be subject to any investigations of the calls or messages. Be aware that sometimes children find themselves caught up in situations that they might not identify as bullying – maybe they were party to "banter" within an online group that was intended as a "joke" but in fact had a negative impact on the target. Encourage children to be "upstanders", not bystanders in such situations by telling a trusted adult if they witness conversations or content that makes them feel uncomfortable or if they can see that it has upset others.

There are a lot of resources out there to help and provide guidance on cyberbullying including the HSE website<sup>9</sup>, Webwise<sup>10</sup> and CyberSafeKids<sup>11</sup>.

#### Illegal images and video clips

Digital technologies have been used to create and distribute videos and images of child abuse and pornography. These are illegal. If you suspect that any image or video you or your child has received is illegal, report it immediately to the Gardaí and report it online at www.hotline.ie.

Hotline.ie will work with the Gardaí to investigate the images or video clips. The Child Trafficking and Pornography Act, 1998 makes it illegal for anyone to produce, forward, publish, send or possess any child



pornography in Ireland. Each mobile operator's website has information on how to report illegal images and videos. Links to this information can also be found on www.hotline.ie.

An Garda Síochána signed a Memorandum of Understanding with the following ISPs: BT Ireland, eir, Sky Ireland, Tesco Mobile, Three Ireland, Virgin Media Ireland and Vodafone Ireland to block access to websites containing child sexual abuse material. https://www.garda.ie/en/about-us/our-departments/office-of-corporate-communications/press-releases/2020/february/internet-sites-containing-child-abuse-material-to-be-blocked-10th-february-2020.html

Bullying can potentially be a criminal offence. If your child has received threatening messages, you should contact the Gardaí. All mobile operators work in co-operation with the Gardaí at their request in cases where bullying has been reported.

- 9 https://www2.hse.ie/wellbeing/mental-health/cyberbullying.html
- 10 https://www.webwise.ie/category/parents/advice/
- 11 https://www.cybersafekids.ie/a-whole-school-community-approach-to-bullying-prevention-and intervention/ or https://www.cybersafekids.ie/tackling-cyberbullying-as-a-cultural-movement/

#### **Top Tips**

Below are some tips and advice you can give your child if they experience cyberbullying or malicious communications:

- Only give their mobile phone number to people they trust. Do not publish their number on a public forum such as the internet, where anyone can see it;
- When signing up to online accounts, always use an email address in preference to a phone number if given the choice;
- Do not reply to abusive or rude text, picture or video messages. Also, do not forward any such messages as they could be assisting a bully or breaking the law;
- Keep a note of the dates and times of any abusive messages and calls, save the messages to their mobile phone (even taking a screen shot of abusive material is advisable), and always tell a parent or a trusted adult such as a teacher;
- Do not send messages to someone when angry or upset;
- Request that their operator provide them with a new mobile phone number if they are being bullied or harassed. The operator can, where appropriate, provide the new number free of charge;
- If bullying is happening through a particular app, then use the block and report functions.

## How you can help keep your child safe

You can take control. It is extremely important to ensure that the account is set up in a way that allows the parent to control the account and the services available. The first step in taking control, is to ensure the account is registered in the parent's name.

By having control of the account parents can check the numbers their child has been calling and texting, and in the case of prepay to manage the amount of money their child is spending on credit. It also allows parents to ask the operator to block or bar certain services from their child's mobile phone subscription, e.g. internet access and some premium rate services. Before purchasing a mobile for your child, check the access and authorised contact services provided by your mobile provider.

Education is a key strategy to empowering and protecting your child online. One really helpful way of educating children is talking to them about what they might encounter online: encourage critical thinking and talk to them about how content and people they come across online may not be what they seem; ensure there are regular check-ins so you can keep an eye on what they are doing and encourage them to come to you if something is troubling them.

The use of parental controls can also be a really helpful strategy in ensuring inappropriate content is filtered out

and appropriate limits are put in place. These are not always fool proof however, and should only be used as one part of a more holistic approach.

#### **Parental Controls**

Parental controls help you manage and restrict what your kids can see and do online – from sites they can view, to the apps they can download, and purchases they can make. Controls can be especially useful for keeping younger children safer from inappropriate content (and from preventing them innocently incurring high costs on games and more), while also teaching them the skills they need to navigate the online world themselves, once they are given the freedom to do so.

The internet for example allows people to access all kinds of information on almost any topic imaginable. Some of this information – if it is educational, for example - can benefit children. But the internet hosts a lot of information and content that is not suitable for children. Many parents lay ground rules for how their children use the internet on a PC or laptop, e.g. restricting the websites they can visit or setting limits for how long they can spend online. Parents are advised to lay similar ground rules for their child's use of the mobile internet, particularly if they have a smartphone and /or are using WiFi. Ensure you are familiar with and have activated the parental controls available on the various search engines, e.g. Google or Chrome and platforms including YouTube. Even with filtering and blocking solutions applied on the mobile phone, it remains important that parents supervise their child's internet usage. In general, the younger the child, the closer a parent should supervise their internet usage.

Mobile operators provide a means of access to the internet. However they have no control over the nature of content, or services offered through the internet.

Mobile operators do not have all the answers either.

Nonetheless, they are committed to providing information on their websites on the controls that are available; these can be utilised by parents and users to customise

#### **Top Tip**

Many Android devices also allow for additional external memory cards to be inserted in to the handsets. Ensuring you are aware of what is saved on the external memory card (if applicable) is extremely important.

To review the memory card files, just go in to 'My Files' on the android device. You will see multiple different sources of memory for the device. Internal storage relates to the phones internal memory,

SD Card will be the memory card storage. Your child may have pictures, videos and various different files saved within memory card folders. Please note that if your child removes the memory card from the handset you will not be able to view the contents.



14

internet access. They also provide links to important resources with invaluable information about how to stay safe online. Parental control features and tools are now built into mobile phones which makes it even easier for parents to turn on parental controls that will allow them to limit how much time their child spends online. These features also allow parents to restrict their child's access to certain applications or websites which reduces the risk of them coming across malicious, inappropriate or upsetting content.

There are a number of different parental control apps available which facilitate the blocking or filtering of internet access so that access to internet content can be restricted. Parental controls are also increasingly relevant across multiple devices and accounts, especially as gaming online is now so popular. Read below for advice and find further reading on the providers, platforms, and devices your family uses.

#### Mobile phones and tablets

Android (Examples - Alcatel, Huawei, HTC, LG Motorola, Nokia, Oppo, Samsung, Sony, TCL, Xiaomi)
You can limit which apps, games and content can be downloaded and disable features such as location and camera.

#### **iPhone**

There are on/off systems for features such as Facetime, in-app purchases and Safari.

#### Windows 10 Phone (Lumia)

The My Family option lets you restrict the games and apps that can be accessed. The Apps Corner option limits content if your child borrows your phone.

#### **Live Streaming Apps & Internet Safety for Children**

Kids love live-streaming apps. Here's what you should know about them. Live-streaming apps allow users to chat or broadcast to other people in real time. They range from those primarily designed for talking to friends and family, such as Skype, to apps that enable you to share moments in your life with a wider online audience, such as Instagram Stories, TikTok or Facebook Live.

Some platforms even provide users with the ability to have their own channel. Disturbing cases involving livestreaming services, and concern that adults are using some services to groom children, have led to concerns about their safe use.

For a generation of teenagers brought up on shows like 'Made in Chelsea' and 'Love Island', these apps offer them the chance to star in their very own reality show. To put that into context, a 2019 study found that a fifth of UK children's no.1 career aspiration was to be a social media influencer. Used in the right way, they allow children and young people to practice communication and presentation skills which can boost their confidence.

For those who use apps to be creative, by sharing singing or dancing performances for example, they also provide immediate feedback, as many apps offer those watching the chance to ask questions, comment or send positive feedback in real-time.

#### Should I be concerned?

Because live-streaming apps are instant, there is no online moderation. No one is monitoring what your children are doing in front of others, or how those watching are reacting. Putting yourself out there means allowing others to comment on what you do and who you are.

Live streaming with strangers online is inherently risky but your child might not think their online friend is a stranger, and so could be persuaded to do things they would not normally do, such as sharing sexual images.

Adults who groom children will often meet them in moderated or public online spaces and then develop a relationship until they can persuade them to take their communication into a private, unmoderated service.

Even if you do not think that your child is using livestreaming apps, warn them of the dangers of doing so and what they can do to stay safe. Talk in detail about the importance of not giving away too much personal information, whether verbally or visually. As with any online service in which they are interacting with other people, you should also advise them not to disclose anything that will reveal their full name, where they live, hang out, or go to school.

Teach them how to block and report on any service they use – and make sure they have a trusted adult who they can confide in should something go wrong.

#### What can you do?

Take an interest in the apps they use... for example TikTok and YouTube, even apps like Facebook and Instagram, which aren't primarily live-streaming apps, now give users the ability to do just that. Give your children lots of opportunities to tell you if anything is troubling them by asking questions.

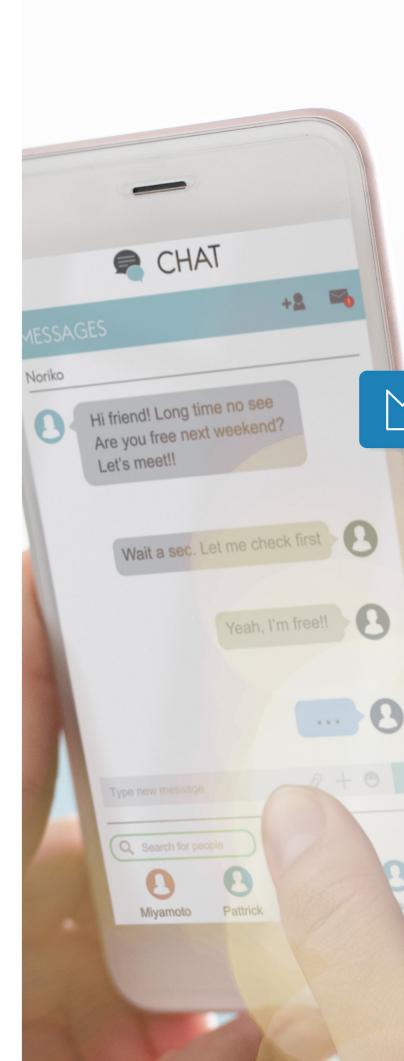
Help them set up privacy settings... limiting the people who can interact with them to those they know in real life. Emphasise to them the importance of not giving away any details...that could allow people to find them in real life, like name, location, school, or address.

#### Make sure they know how to report any

**harassment...** to the app or platform. If an adult makes a sexual approach, they should tell you or another trusted adult and report it to the platform.

Help them to understand and value their data – so many children value popularity over privacy!

<sup>12</sup> https://www.telemediaonline.co.uk/young-affiliates-nearly-a-fifth-of-british-children-aspire-to-be-social media-influencers/



15

#### **Top Tips for Parents**

- Understanding how the technology works yourself is the best way of making sure your child uses their mobile phone safely and responsibly;
- Know where to avail of the most up to date information and guidance – you cannot go wrong by checking the Online Safety Hub, Webwise and CyberSafeKids;
- Make sure the account is registered in the parent's name;
- Contact your mobile provider to check the access and authorised contact services provided.
- Consider internet safeguards available e.g. filtering technologies and apps;
- Encourage your child to talk
   openly about the experiences they
   encounter while using their mobile
   phone. Make it really normal to talk
   about what they are seeing and
   doing online, which will hopefully
   encourage them to come to their
   parents if something goes wrong.
   Sometimes a child will hide a
   negative experience from parents
   because they fear their mobile phone
   or internet access will be taken away.
- Report offensive or illegal calls, messages or images to the Gardaí
- Advise your child not to respond to a call or text if they do not recognise the number
- Take note of the IMEI number on your child's mobile phone so the operator can disable the handset if it is lost or stolen

- Advise children to take care when using their mobile phone in public.
   A mobile phone is a valuable item and can be a target for theft.
- Text 'STOP' to end a premium-rate subscription. Contact ComReg if this fails to work.
- Apply service barring offered by your mobile provider e.g. premium SMS barring.
- Forward suspected spam messages to your mobile operator's reporting line.
- Make your child aware that using a mobile phone in certain places is inappropriate, e.g. a cinema or library.
- The internet is a public place and children can never be sure who is reading the information they publish online. They need to be very careful about publishing personal details.
   Name, address, telephone number, school and location can make a child identifiable in the real world.
- Photographs and information published online are there forever.
   Children cannot get them back and cannot control how other people will use them. Children should think carefully – and ask a parent's approval – before publishing (uploading) any photographs of themselves.
- Do not trust everything they read or are told online. People online can lie. For example, an adult can try to win a child's trust by pretending to be a child themselves. Children should never arrange a real-world meeting with someone they met

- online without first telling a parent or a trusted adult. And certainly, they should never go alone to meet a stranger.
- Encourage your children to talk to you if they receive a message that is frightening, threatening, rude or makes them feel uncomfortable. Reassure them they will not get in trouble by telling you about something negative they encountered on the internet or their mobile phone.
- Children who use a socialnetworking website are advised to set their profile to 'private'. This means only 'friends' can view their personal information. However, children should still be careful about publishing personal information online. Even a profile set to 'private' is not 100% secure.
- Get involved in Safer Internet Day:
   Safer Internet Day (SID) is an EU
   wide initiative to promote a safer
   internet for all users, especially
   young people. It is promoted
   in Ireland by PDST Technology
   in Education and Webwise, and
   supported by industry partners in the
   telecommunications sector. https://
   www.webwise.ie/saferinternetday/
- It is important to talk to your children about keeping friends lists to those they know in person only.

#### Other useful contacts online:

- ComReg, the Commission for Communications Regulation: www. comreg.ie
- Irish Safer Internet Centre: www. internetsafety.ie

- Webwise, provides parents, teachers and children with information and advice about potential dangers online and how to stay safe and secure online: www.webwise.ie
- CyberSafeKids, Established in 2015, CyberSafeKids\* is an Irish registered charity which works to empower children, parents and teachers to navigate the online world in a safe and responsible manner. www. cybersafekids.ie
- Hotline.ie is Ireland's primary channel for members of the public to anonymously, confidentially, and securely report potentially criminal content online, especially child sexual abuse material and activities relating to the sexual exploitation of children i.e. child grooming. www. hotline.ie
- An Garda Siochána: www.garda.ie and https://www.garda.ie/en/crime/ online-child-exploitation/onlinechild-exploitation.html
- Media Literacy Ireland: www.medialiteracyireland.ie
- Be Safe Online is the government's campaign to highlight ways to help you stay safe online – it provides access to a wide range of online safety resources, to support online safety for all. It is Ireland's official online safety hub: https://www.gov. ie/en/campaigns/be-safe-online/
- HSE provides important information on mental health and wellbeing: www.hse.ie and here https:// www.hse.ie/eng/services/list/2/ primarycare/childrenfirst/children. html

18 19

### Glossary

#### **Bill Pay**

Customers pay after they have made calls, sent texts, or used another mobile service. They will have a signed contract with a mobile operator, e.g. for 30 days, one year, 2 years and will receive a bill at the end of each month. Customers must be at least 18 years old to sign a contract with a mobile operator.

#### **Bluetooth**

Bluetooth is one of the technologies that enables devices to connect wirelessly, for example a mobile phone can send data (e.g. pictures) to another Bluetooth enabled device i.e. another mobile phone, printers, tablets, TVs, headsets, smart watches etc. If your child's mobile phone has Bluetooth they can switch it on and make a private connection to a friend's phone. They can then swap information, e.g. pictures or videos, across this private connection. Bluetooth is popular among children because establishing the connection is easy. It is also free and does not use data allowances.

Bluetooth can be used only when two devices are physically close to each other, in the same room or building. Bluetooth can be switched on or off. Children are advised to switch off Bluetooth when they are not using it. If it is left on, other people nearby can try to connect to their mobile phone and send them unwanted messages.

#### **Email/webmail**

Email is short for electronic mail. It allows you to write, send and receive messages across the internet. Instead of calling a number, you reach people through their email address. Each email address contains a symbol – @ – known as the 'at' sign, e.g. johnsmith@icia.ie. To send an email you will usually use a computer program such as Microsoft Outlook and webmail services. Examples of webmail include Hotmail, Yahoo mail and Gmail, and these can also be accessed on a mobile phone.

#### Geotagging

With location settings on, any photo or video is created with location and time information stored within the file. This information is contained within any image or video posted online and can be easily extracted by anyone who knows how to do it, and if content is being posted in real time, then you are potentially giving away your physical location to strangers.

#### **GPS (Global Positioning System)**

A system by which signals are sent from satellites to a special device, used to show the position of a person or thing on the surface of the earth very accurately.<sup>13</sup>

#### International Mobile Equipment Identity (IMEI)

This is the unique serial number that every mobile handset comes with. It can be found behind the battery in your handset or accessed on most mobile phones by keying in \*#06#. If your handset is lost or stolen, you can have it disabled by calling your mobile operator and quoting your IMEI number. Once reported and disabled, the mobile phone cannot then be used.

#### **Networks**

Mobile phones operate over a radio wave system using a network of mobile phone masts. Just as the phones themselves are constantly being updated to deliver faster, better quality services, so is the network of masts.

#### OTT (Over the Top) Services

Over the Top (OTT) services are a popular way for people to communicate. OTT services are delivered via an internet connection, rather than through calls or SMS (texts). Facetime, Instagram, Messenger and WhatsApp are all examples of OTT apps. These apps can be used to send and receive messages and conduct voice and video calls. These services are considered by mobile operators to be data services and will be charged as part of your child's data allowance if used on a network connection. A mobile phone without a SIM card can still use these data services because they only need a Wi-Fi internet connection.

#### **PRS (Premium Rate Services)**

Many people like to 'personalise' their mobile phone. This can mean adding pictures and sounds to the handset that matches their personality and interests. For example, children can use a short clip of their favourite song as the sound (tone) their mobile phone makes when it rings. This is often called a ringtone. Children can personalise their mobile phone by buying 'content', e.g. ringtones, photographs or logos. They can also sign up (subscribe) to receive interesting information or enter competitions. Such content and information are purchased through premium-rate services (PRS).

#### **Prepay**

Customers buy credit, for example, online or physically in a shop. They then 'top up' or add the value of the credit to their mobile phone account. These customers pay before they make calls, send texts, or use another mobile service. Children are most likely to have a prepay account.

#### SIM card

The SIM card provides you with your phone number. It also includes a unique microchip which you can use to store information: for example, your address book, sent or received text messages, numbers you have dialled, and calls you have received. If you move the SIM card to another handset, all the information stored on it goes with it.

To send and receive calls or texts, a mobile phone needs a SIM card. This is short for Subscriber Identification Module card. The SIM card, in many ways, gives the handset its identity as your mobile phone. When someone calls your number, it is the SIM card that tells the mobile phone to ring. That is because the SIM card carries the information on your mobile phone account, including your number. If you take the SIM card out of your mobile phone it will not ring when someone calls you. If you place your SIM card into another mobile phone, that phone will ring when someone calls your number.

#### **Smartphones**

All modern mobile phones can take photos and make videos. The photos or videos can immediately be sent to another compatible smartphone, to an email address or shared online. They can also be stored on the phone or transferred to a personal computer.

#### **SMS (Short Messaging Service)**

SMS or text messages. These are messages sent over the operator's network, not over an internet or Wi-Fi connection.

SMS can also be used to buy ring tones, receive information, or to vote – for instance in TV reality shows. These services are called premium messaging services and are explained above in the PRS section.

Messages can also be sent using messaging applications such as WhatsApp or Messenger and these are sent over the internet using mobile or Wi-Fi data.

#### Spam

Spam is the term used for unsolicited email or text messages. Spam usually comes from third parties promoting a new product or service and can include links to adult content or websites. Some messages may announce that you have won a prize and should ring or text a certain number to claim it. This may promote a premium rate number and could involve a high cost premium SMS or a long call, at the end of which you may discover the prize is worth far less than the cost of claiming it.

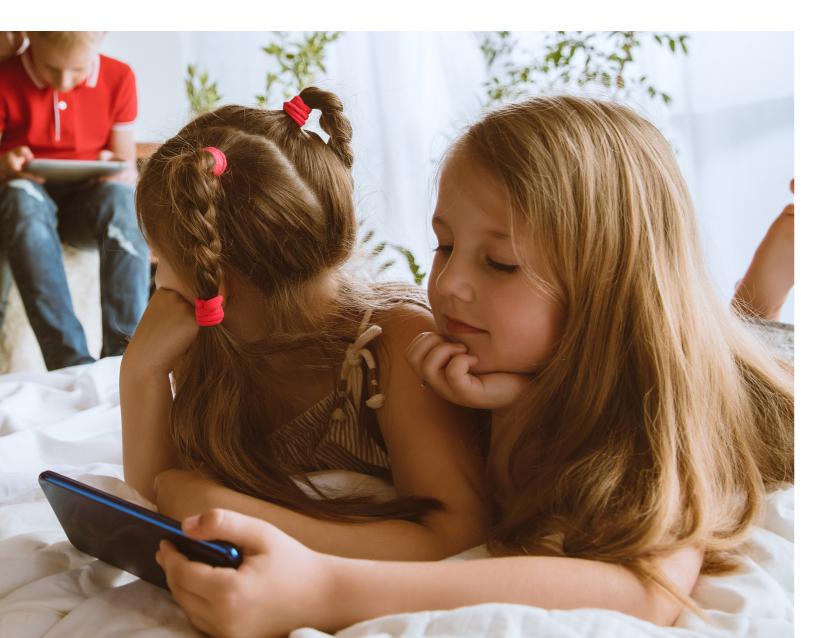
Often children are not able to differentiate between what is advertising and what is not. In particular, children can be easily enticed into responding to messages that promote prizes or free products.

13 https://www.oxfordlearnersdictionaries.com/definition/english/gps?q=gps

20 2

## Code of Practice

All the Irish mobile operators mentioned in this document have signed up to Telecommunications Industry Ireland's Code of Practice for the Responsible and Secure Use of Mobile Phones which establishes the standards which mobile operators will adhere to on issues such as parental controls, malicious communication, internet access, spam and premium-rate services.





84/86 Lower Baggot Street, Dublin 2. D02 H720. www.ibectii.ie

