

# The Digital Inclusion Handbook

---

Core computer literacy for beginners

Author  
**Alex Rowley**





March 2022

**Author:** Alex Rowley (Wavemaker Stoke)

## Copyright

© Alex Rowley has asserted his right under the Copyright, Designs and Patents Act 1988 to be identified as the author of this work. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior permission of the copyright owner.

## Disclaimer

All the guidance, ideas and suggestions included in the content of this guide are intended to inform readers about how to use digital technologies in their own home or other setting. The content is not a substitute for national advice and guidance from professional or regulatory organisations. While every effort has been made to include accurate and up to date information, knowledge and understanding of assistive technology are constantly evolving and being updated. So you need to use the content of the guide to learn more about how you can adopt or enhance your use of digital technology and weigh up the choices, information and guidance for your own circumstances. Inclusion of named agencies, websites, companies, services or publications in this book does not constitute a recommendation or endorsement. Any professionals using this guide in signposting service users to use digital technology for themselves, must endorse national requirements relating to IT security, data protection and privacy, information standards.

## About Wavemaker

Wavemaker is a digital skills training provider. We provide training and skills engagement for key skills for the future, such as digital design and coding. We also work to increase digital literacy, sharing skills, teaching knowledge, and building confidence.

We are also involved in enabling the use of technology within the healthcare sector, working from both the clinical and patient perspective.

## About the author

With a professional background spanning over 20 years, Alex has a significant amount of experience with technology. His skills encompass a wide array, from the technical aspects of networking infrastructure, equipment deployment and management, to training, support, advice and guidance. Furthermore, Alex's digital and graphic design skills, twinned with a high attention to detail, help to bridge these key areas when working with a client.

As one of the Directors of Wavemaker, Alex has an in-depth knowledge of the challenges that relate to the education and training sector. He is passionate about helping to steer change, both as an individual and as a representative of Wavemaker. The organisation's core aim is to empower individuals with the knowledge, skills and confidence needed to utilise technology in order to enhance and improve lives.

# Contents

<b>Introduction</b>	<b>4</b>
<b>Getting online</b>	<b>7</b>
<b>Staying safe online</b>	<b>8</b>
Passwords	8
Email Scams	10
Fake Social Media Profiles	10
Compromised Social Media Profiles	11
Non-Secure Websites	11
<b>Shopping online safety</b>	<b>11</b>
The risks	12
How to check if a website is safe	12
Try to use trusted retailers	12
Does the website accept credit cards?	12
Look for an address and phone number	12
Be suspicious of deals that are too good to be true	13
Check out the reviews	13
Check for an SSL Certificate	13
Check for a privacy statement	13
<b>Online banking safety</b>	<b>14</b>
Choose an account with two factor authentication	14
Create a strong password	14
Secure your computer and keep it up-to-date	15
Avoid clicking through emails	15
Access your accounts from a secure location	15
Always log out when you are done	16

Set up account notifications (if available)	16
Monitor your accounts regularly	17
<b>Apps</b>	<b>17</b>
Installing and staying safe with apps	17
App Store overview	18
<b>Email</b>	<b>19</b>
How to set up an email address and send an email	19
Signing up to Google email (Gmail) on a desktop or laptop computer	20
Signing up to Google email (Gmail) on a tablet or smartphone	24
How to send, reply and forward an email with Gmail on a desktop or laptop computer	26
Replying to and forwarding a message	28
Sending an email with Gmail app on a tablet or smartphone	29
Gmail app overview	30
Sending emails	30
<b>Social media</b>	<b>31</b>
Facebook	31
Signing up to Facebook on a desktop or laptop computer	32
Signing up to Facebook on a tablet or smartphone	34
Accessing Facebook groups and viewing pages on a desktop or laptop computer	37
<b>Video Calling</b>	<b>39</b>
Equipment	39
Software	39
<b>Messaging Apps</b>	<b>40</b>
Overview of WhatsApp on a smartphone or tablet	41
Groups	42
Joining a WhatsApp group on a smartphone or tablet	42
<b>Jargon Buster</b>	<b>43</b>
<b>Password Passport</b>	<b>47</b>

# Introduction

This guide has been created to support people in fundamental use of computers and smartphones. It is intended for people who may have limited experience of computers and similar digital devices.

The guide offers a mix of how-to instructions and general guidance, and covers a range of different topics including email, online banking, being safe online and social media.

The guide is written with the perspective of using a desktop or laptop computer. However, all skills are transferable and may only appear visually different when using a smartphone or tablet. Additionally, handheld devices tend to offer a more intuitive experience, and often guide you step-by-step through core processes.

## Desktop, laptop, smartphone or tablet - what's the difference?

There are so many options today about what kind of computer you should use, and the simple answer is - any. All have their pros and cons which we'll briefly touch on in this section, but ultimately, they will all allow you to engage in the digital world, keeping us better connected and helping us to enrich our lives.

Traditionally, computers are found in a desktop or laptop form. In more recent years, there have been increasing technological advancements in handheld and mobile devices, which have offered new ways of interfacing [interacting with them] over the traditional mouse and keyboard.

Desktop computers are made up of separate peripherals [or components] such as a base unit, monitor, keyboard, mouse and speakers. Additional items such as a microphone and webcam may be needed if you plan on using it to make video calls. Desktop computers are often controlled with a keyboard and mouse.

Laptop computers encompass all of this technology within one package, and often including the webcam and microphone embedded in the case. A portable alternative to a desktop computer for someone who needs the capabilities of a desktop computer and the ability to easily move it about. Laptops offer an alternative to a mouse in the form of a trackpad, allowing you to point and click using your finger.

Both desktop and laptop computers are still considerably more powerful than smartphones and tablets in terms of processing power [brain power], RAM [short term fast access memory] and storage space [long term memory]. However, this is only a factor if you were to plan on using an advanced piece of software such as 3D design, animation rendering or complex mathematical **simulations** which can all be intensive on these resources.

The majority of smartphones and tablets now have the power needed to perform many tasks quickly and efficiently. Handheld and mobile devices perform many of the functions of a computer, such as browsing the internet, sending and receiving email, and running software applications [apps].

Unlike desktop computers and laptops, smartphones and tablets make use of a touchscreen to allow you [the user] to interact with the phone and installed applications.

Smartphones and tablets are generally designed to be used on their own without any additional devices. This means smartphones have all the important devices built-in to them such as cameras, microphones and speakers, as well as a display screen.

The following tables compare various aspects of desktops, laptops, smartphones and tablets.

Interaction	Desktop	Laptop	Smartphone	Tablet
Navigation	Mouse	Trackpad or mouse	Touch screen or stylus	Touch screen or stylus
Typing	Full size physical keyboard	Integrated physical keyboard	Small touch screen keyboard	Touch screen keyboard with an option for add-on wireless keyboards.
Display	External Monitor	Built-in monitor	Built-in display screen	Built-in display screen
Listening	External speakers	Built-in speakers	Built in speakers	Built in speakers
Hearing (microphone)	External microphone	Built-in microphone	Built-in microphone	Built-in microphone
Seeing (camera)	External camera	Built-in front facing camera	Built-in front and rear facing cameras	Built-in front and rear facing cameras

## Operating Systems (OS)

An operating system (OS for short) is the core software application on a device, and the first thing you see and interact with when you switch it on. The OS communicates with the device's hardware, such as the keyboard, mouse, display and the Wi-Fi. In other words, an operating system handles input and output devices.

Applications can be installed onto the operating system. The OS therefore sits in between the hardware and the application, and in essence, negotiates the transaction happening between them. For example, when you want to print a picture, the application you are



using will liaise with the OS, which will then take that instruction to the hardware, a printer on this occasion.

Having this core understanding when using your device can allow you to diagnose a fault when an error occurs. Depending on the kind of error you are experiencing you can begin to determine what is at fault - whether it is app specific or a wider system problem (OS or hardware).

For example, if a problem occurs and you are unable to print, the first focus would be that either the printer hardware, or the device connection [to the printer] is the problem, not the application.

Now, if the problem you experience is related to a unique feature on an app then you can quickly determine that the app is where the fault lies.



### Security tip

No matter what device and operating system you are using, make sure you keep it up-to-date. Software and OS updates are regularly released to fix bugs, glitches and security holes, so check from time to time and keep updated!



# Getting online

## Accessing the internet

The Internet is a global network that connects computers anywhere in the world. Through the Internet, people can share information and communicate, often through websites and email.

A website is a collection of web pages and related content that is identified by a common domain name, otherwise known as a **web address** or **URL**.

All devices use a web browser to access the internet, although, experiences will differ depending on what you are using. When using desktop or laptop computers, a browser [*also referred to as a **full browser***] allows you to engage in all of the website features.

Due to display and power constraints on mobile devices, user interface and user experience may differ and some features may not function correctly. In response to this, many companies and websites offer a specific app to access their services. This allows them to offer the full functionality which may be missing when viewing through a mobile web browser.

Popular internet browsers in use today are Google **Chrome**, Microsoft **Edge**, Mozilla **Firefox** and Apple's **Safari** browser.

No matter what internet browser you use, all core features and functionality remain very similar.

### Address bar

This is where you type the address off the website you wish to visit.

This also doubles as a search bar to allow you to look up any key words (e.g, business, places and people).

### Close / Minimize / Maximize

These apply to and allow you to control the browser window you have open.

### Navigation buttons

Forward and back buttons allow you to navigate through the page. If someone says "click the back button", this is what they are referring to.

### Refresh button

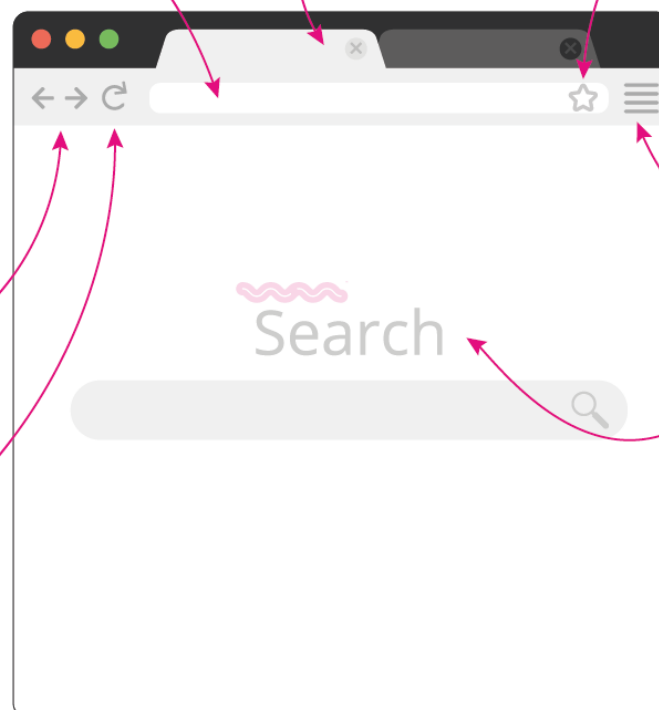
Click this will reload the webpage. Sometimes you have to do this if the page does not display correctly.

### Tabs

These are different pages or sites that you can have open.

### Favourite button

The **star** will allow you to add a bookmark of the site you are on.



### Menu

Here you will find options for the browser, such as **New Tab** or **Window**, **Print**, or **Settings**.

### Content pane

This is where the website will be displayed.

# Staying safe online

## Passwords

Many people struggle with choosing a password. You want a password that you will remember but that a hacker won't be able to figure out. Here are some tips on creating a secure password.

Before we go into further details, it is important to note that you should not use the same password for all of your accounts, the most important of which is your email account. If this account is compromised then a hacker could use that to gain access to your other accounts, by requesting a password reset. Think of your email account as a master key to all of your other online accounts.

In an ideal world you would use a unique password for every account you have, but in practice that is hard to manage and remember. Therefore we recommend that you categorise your accounts into groups, using the same password for all the accounts in the group, but a different password per group. That way, if one of the sites you use has a data leak and your password is exposed, you only need to change the passwords on the accounts that are in the same group.

Example groups:

Group	Description
Group 1	Email account
Group 2	Well known [trusted] e-commerce sites such as eBay, Amazon,
Group 3	Social media accounts
Group 4	Media streaming services such as Spotify and Netflix
Group 5	Any other accounts

## Avoid obvious passwords

Some of the easiest passwords to remember are also some of the least secure. Try to avoid using passwords that are also:

- Your partner's name
- Your child's name
- Your pet's name
- Your address

While these types of passwords are easy to remember, the information is also fairly simple for a hacker to find out. In some cases, such as your address information, it may even be public record.

If a hacker manages to get into your social media account, they can probably also learn the names of those close to you.

Passwords that others commonly use are also bad choices. They are among the first that a hacker would try to gain access to your account with. Some of the worst passwords that people use (and that should be avoided) are:

- 123456
- abc123
- password
- welcome
- letmein

## Choose a longer, random password

The best passwords are random and contain various types of characters. For example, a password that contains upper and lowercase letters, numbers, and symbols is harder to hack than a password of all letters or numbers.

Also, the longer the password, the harder it is to hack. Passwords should be at least eight characters long. Some experts recommend using twelve or more characters.

Avoid stand-alone online password generators since the site may be trying to harvest passwords.

Once you find a good password, you may be tempted to use it for all your accounts. Don't do this. If your password becomes compromised, then the hacker potentially has access to your entire online presence.

## How to store your passwords securely

Some of the characteristics that make your password hard to guess, also make it harder to remember. That's why it's important to come up with a secure way to store your passwords.

Having a secure password is no good if hackers can easily find it. Whenever possible, avoid:

- **Using your email password on a public computer.** If you do use your password on a public device, clear the cache and memory afterwards. You may also wish to change your password.
- **Keeping your password on your person.** Writing your passwords on a slip of paper and keeping it in your wallet can be a problem if your wallet is lost or stolen.
- **Storing your password in an unprotected document.** It's common for users to create Word or Excel password lists. This is not a secure practice. The trouble is, anyone who accesses your machine can open these documents.

Using a reliable password manager can be a safer option to help you keep track of all those passwords. Password managers use encryption and other means to keep your data safe.

## How often should you change your password?

While the motivation behind regular password changes is good, some studies have shown that they are less than effective. That's because the majority of users don't create totally new passwords when they change their password. Instead, they simply change their current password by adding or changing a character.

Experts suggest that choosing a strong password is a better security tactic than frequent password changes. It's important to select a strong password to begin with.

Below are the most common dangers that we all fall prey to. Be aware and think twice before acting.

## Email Scams

Email scams are similar to mailed letter scams, but digital. With email scams, people pretend to be legitimate companies wanting something from the recipient. For example, a sweepstakes company sending you an email saying that you won the grand prize and asking you to pay a fee. Scammers can also pretend to be a loved one looking for money. Thankfully, most scam emails end up in the Spam folder, but sometimes they do end up the Email Inbox.

## Fake Social Media Profiles

On Social Media, there are people who create fake profiles for the purpose of spreading false information (spammers), leaving fake reviews, and scamming others. Fake accounts are often used to trick people into handing over information or even money.

Sometimes, it can be as simple as accepting a friend request that can leave you vulnerable.

There has also been an influx in 'bots' over the last few years focusing on spamming false information or political agendas. A bot is a software program that operates on the Internet and performs repetitive tasks.

To protect yourself, always be vigilant when using social media and accepting friend requests or believing information. You should not friend and follow anyone you don't know, unless it's a verified account of someone or an organisation that you trust.

If you're unsure then view the user's profile and check:

- Does the account have a profile photo?
- Does the profile name seem legitimate?
- Is the account more than just a few months old?
- Does the account have more than 25 friends or followers?
- Is the account creating a range of different content?

If the answer is "No" to any of these questions then the profile might not be real. The more "No" answers, the higher the likelihood the account is fake.

## Compromised Social Media Profiles

As a progression to creating and using fake profiles on social media, spammers and hackers have adopted a new approach in recent years where they gain access to, and take control of, someone else's user account. As with fake profiles, they will then use this to spread false information (spammers), leave fake reviews, and scam others. The difference between the two is that a compromised account often offers more legitimacy as it would have been genuine until it was compromised, with past posts and photos from when the account was in control from its original user.

Victims losing control of their accounts often do so due to the poor password and security they have implemented. It could also be down to only one or very few passwords across many of their online accounts. Once one of these accounts or websites is compromised, or has a data leak, then it leaves all other accounts using the same password vulnerable.

## Non-Secure Websites

Sadly, not every website on the internet is secure and safe to use. Non-secure sites could hold all kinds of trouble from hackers to malicious malware. An easy way to spot a non-secure site is looking at the beginning of the URL. If it begins with 'https', then it's likely secure. However, if it begins with 'http', the site is likely to be unsafe. Another way is having anti-virus software installed on your computer. Certain software programs like Norton Security have safe search which notifies users of a site's safety level.

Being aware of these online safety basics and dangers will keep seniors protected online. If you have elderly parents, an easy way to monitor their online activity is by using a spy phone application.

# Shopping online safety

Online shopping (e-commerce) is generally safe. Security measures have improved considerably since the early days of the Internet, where a lack of encryption and security regulations made Internet shopping risky.

In 2002, a set of e-commerce regulations came into force in the UK that offered greater safety to online consumers. These regulations apply to any online retailer of any size and require the disclosure of various details, including the name of the service provider, the address of the provider, contact details of the business, a registration number and VAT number. However, there are still some risks.

## The risks

The risks for online shoppers out there, with fraudulent websites and data leaks remaining a persistent problem. Online consumers are more at risk of accidentally buying fakes or replicas online due to trusting a photograph rather than inspecting the item in real life. Purchasing items that don't match the description, or goods that are damaged or unsuitable, is also a risk when it comes to making online purchases.

If you are browsing the web using an unsecured Internet connection, such as a free Wi-Fi hotspot in a public place, then try to avoid making any online purchases. Public Wi-Fi is more vulnerable to attack by hackers or malicious software and could put you at an increased risk of fraud, so try to save any retail therapy for a night in.

## How to check if a website is safe

There are many clues to identify whether a website is safe before making a purchase. Below are the features to be aware of when performing due diligence on ecommerce websites:

### Try to use trusted retailers

If possible, try to buy from retailers you have heard of, especially those with a reputation for customer service. If you're looking for a specialist item that is only available on an independent website, be as diligent as possible before handing over any financial information.

Frequent spelling or grammatical errors in the product descriptions or website copy can be a good indication as to the quality of a website. Websites that appear to be written in broken English should be avoided, as well as websites that don't include unique photographs of the product, the ability to leave reviews, or an advertised returns policy.

### Does the website accept credit cards?

Credit cards are the safest method of making online purchases, as it's easier for credit card companies to refund any money lost due to fraud. Websites that don't accept credit cards should raise a red flag, as it's often more difficult for fraudulent websites to become certified by credit card companies.

### Look for an address and phone number

Legitimate retailers almost always have a contact number and physical address visible in the header or footer of the website. If you have any reservations about the legitimacy of a website, copy and paste the address into a search engine to see if the given location is accurate. This is a good indication of a legitimate website, as unreliable sellers will often be online only to avoid detection, or use a fake address.

## Be suspicious of deals that are too good to be true

If something seems too good to be true, then it probably is. Be cautious of any website that appears to be selling well-known brands of designer items for considerably less than the retail price. If you discover a website that stocks popular items for very low prices, there's a risk you're handing over money for fakes or replicas.

Common sense is usually enough to avoid being misled by these pitfalls. We also recommend searching for the same item at different retailers to give you a greater awareness of the average price.

## Check out the reviews

While these tips can give you practical visual clues to look out for, reviews and personal accounts from other users are an excellent way of staying safe while shopping online.

Websites like <https://uk.trustpilot.com/> can be a useful resource when looking for further information about a website you haven't used before – it's a great place to read reviews and personal experiences concerning a huge variety of online retailers.

## Check for an SSL Certificate

An SSL Certificate is also a good indicator of trust and legitimacy on a website. There are two easy methods of determining whether a website has SSL certification. Firstly, an icon of a locked padlock should be present in the URL bar at the top of your web browser. Another method of identifying a website with an SSL certification is the domain name:

- Secure websites begin with: `https://`
- Unsecured websites begin with: `http://`

### What is an SSL Certificate?

An SSL (secure sockets layer) is an encryption method that all online retailers who deal with credit or debit card details must have. An SSL encryption stops hackers from accessing your personal or financial information, ensuring your details are secure and safe.

## Check for a privacy statement

Look out for a privacy statement on any website you are planning to make a purchase from. A privacy statement detailing how the business collects, uses, and protects sensitive financial information should be readily available from any retailer – so if you're struggling to find one, this could be a bad sign.



# Online banking safety

Online banking is convenient but it does come with certain risks. Just as you hear of people being robbed at cash machines, or having their cards cloned, so online accounts are also a point of vulnerability.

It doesn't have to be scary or risky though. Here are some tips to help you minimise the risks to your finances, and to bank safely online.



## Note

**Banks and building societies all have their own methods of security, so all of the tips and advice below may not apply to your account.**

## Choose an account with two factor authentication

Try to get a bank account that offers some form of two factor authentication for online banking.

**Two factor authentication**, or **2FA**, is an extra layer of security used to make sure that people trying to gain access to an online account are who they say they are. First, a user will enter their username and a password. Then, instead of immediately gaining access, they will be required to provide another piece of information. This is commonly sent via a text message, or verification email. Sometimes you'll be given a link to click, other times you will get a code to enter.

These days many, but not all, banks offer a small device that can be used to generate a unique code each time you log in. This code is only valid for a very short period of time and is required in addition to your login credentials in order to gain access to your online account.

## Create a strong password

If your bank requires a user-generated password in order to access online accounts make sure that you choose one that is strong. The best way to achieve this is by making it long and a mix of upper and lower case letters, numbers, and special characters.

Always avoid using any common words or phrases and never create a password that contains your name, initials, or your date of birth.

When setting up online banking, if your bank asks you to provide answers to some standard security questions, remember that the answer you give doesn't have to be the real one.

So you don't have to answer "Poochie" to the name of your first pet – you can make it something else as if it was a password. **But you must remember your answer.**

## Secure your computer and keep it up-to-date

Security software is essential these days, regardless of what you use your computer for.

As a minimum, make sure you have a firewall turned on and are running antivirus software. This will ensure you are protected from Trojans, keyloggers and other forms of malware that could be used to gain access to your financial data.

You'll also want to keep your operating system and other software up-to-date to ensure that there are no security holes present.

## Avoid clicking through emails

No bank or building society will send you an email asking you to provide any of your login details.

If you receive an email that appears to be from your bank that asks for such details then **treat it with suspicion** as it may well be a phishing attempt to trick you into handing your credentials over.

Likewise, be aware of links in emails that appear to be from your bank – this is a trick often employed by the bad guys to get you onto a website that looks like your bank. When you log in to 'your account' they will steal your username and password and, ultimately, your cash.

It is always safer to access your online bank account by typing the address into your browser directly.

Also, be aware of unsolicited phone calls that purport to be from your bank. While your financial institution may require you to answer a security question, they should never ask for passwords or PINs (personal identification numbers; they may ask for certain letters or numbers from them, but never the whole thing).

If in doubt, do not be afraid to hang up and then call your bank back via a telephone number that you have independently confirmed as being valid.

## Access your accounts from a secure location

It's always best practice to connect to your bank using computers and networks that you know and trust.

But if you need to access your bank online from remote locations you might want to ensure your connection is secure. Look for a small padlock icon in the address bar on your internet browser, and also the address; the URL of the site you are on should begin with '**https**'. Both act as confirmation that you are accessing your account over an encrypted connection.

## Always log out when you are done

It is good practice to always log out of your online banking session when you have finished your business. This will lessen the chances of falling prey to session hijacking and cross-site scripting exploits.

## Set up account notifications (if available)

Some banks offer a facility for customers to set up text or email notifications to alert them to certain activities on their account. For example, if a withdrawal matches or exceeds a specified amount or the account balance dips below a certain point then a message will be sent.

Such alerts could give quick notice of suspicious activity on your account.

## Monitor your accounts regularly

Monitoring your bank statement each month is good practice as any unauthorised transactions will be sure to appear there.

But why wait a whole month to discover a discrepancy? With online banking you have access 24/7 so take advantage of that and check your account on a regular basis. Look at every transaction since you last logged in and, if you spot any anomalies, contact your bank immediately.

# Apps

An **app**, also referred to as an **application**, is a computer program designed to run on a mobile device such as a smartphone or tablet.

There are many different categories for apps, from productivity tools to games. Some websites or businesses also have their own app to allow you to access their services in an efficient easy way.

Unlike traditional computers, where software applications would be purchased on disc or downloaded and then installed manually, apps are only available through **application stores**, or **App Store**. An App Store is a digital distribution platform that is accessible through an internet connected smartphone or tablet. Depending on the make of the device you use, the stores may differ slightly - but are still very similar.

There are two main App Stores you could encounter on a mobile device, those being the **Apple's App Store** on iOS and **Google's Playstore** on Android OS.

The advent of app stores have helped ensure only genuine apps are available for install, offering assurance of downloading trustworthy apps from verified mobile developers.

Despite this, we still find bad apps out there and should always check the information about an app before downloading it.

## Installing and staying safe with apps

To install an app, you would visit the app store available on your phone and use the search feature to look for what you want. You can either type the specific name of an app if you know it, or you can search keywords or categories. On tapping search you will be given results.

Questions to ask yourself before downloading an app are:

- Do you recognise the publisher?
- Does it have a good rating?
- Are there any user reviews?
- Does it offer in-app purchases?

*(In-app purchases are extra content or subscriptions that can be bought from inside an app. Not all apps offer in-app purchases.)*

Reviewing this information before downloading an app can help you to decide whether the app is right for you.

Here is an example from the Apple App Store on how it looks, and what to look out for when searching for apps.

## App Store overview

The diagram illustrates the Apple App Store interface with two screenshots and several annotations. The left screenshot shows the main App Store home screen, and the right screenshot shows the search results for 'facebook messenger'.

**Account & settings**  
 Here you can access your account information, and payment details (if you want to purchase apps).


**Content window**  
 This will display the relevant content for the menu being viewed, or search term entered.

**Menu bar**

**Search bar**  
 Type in the name of an app or a topic that you want to search for.

**Search results**  
 This will display the apps that fit your search criteria.  
 Tap an app to find out more information.  
 Get to download and install.

**Search menu**  
 Tap this to begin.



**App name**

**Publisher**

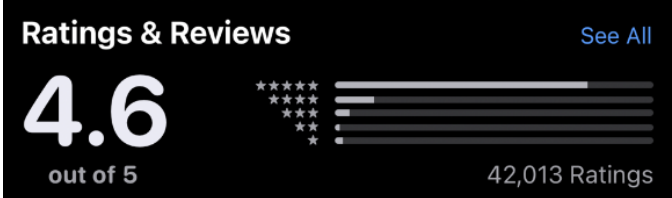
**Download /Install**

**Core information**

**Content window**  
This will display the relevant content for the menu being viewed, or search term entered.

**Menu bar**

Scroll down to see user reviews and other information such as in-app purchases (what they are and how much).



**Ratings & Reviews** [See All](#)

**4.6**  
out of 5

42,013 Ratings

# Email

An email [or electronic mail] address is a unique identifier for an email account. It is used to both send and receive email messages through the Internet. Messages can also include attachments, such as documents, photos and videos.

Like physical mail, an email message requires an address for both the sender and recipient in order to be sent successfully.

All email addresses have two main parts: a username and a domain name.

The username comes first, and is something you can choose. This is followed by an at symbol [@], and then by the domain name. The domain name is linked to the email service provider, for example, @outlook.com

In the example below, '*alex*' is the username and '*wavemaker.org.uk*' is the domain name.

**alex@wavemaker.org.uk**

## How to set up an email address and send an email

Emails can be created with a wide variety of service providers. All are alike and offer very similar services. We ourselves use Google as they are a large company who appear to follow all the

correct policies and security measures, and ensure we are kept safe. We trust them to keep our information and data private.

A Google account also allows you to access Google's other services, such as Google Drive (an online internet based data storage solution, offering 15GB of Cloud storage for free), YouTube, and the Play Store (Google smartphones and tablets)

Other good email providers include Microsoft with their Outlook email service, and Apple with their iCloud services. Although the latter is more often associated with Apple products.



## Signing up to Google email (Gmail) on a desktop or laptop computer

1. To sign up for Gmail, create a Google Account by opening an internet browser and going to the Google account creation page:

<https://accounts.google.com/signup>

2. Complete the form with your:

- **First name**
- **Surname**
- **Username**
  - This can be anything you want it to be, providing it hasn't already been used.
  - You won't be able to get a certain Gmail address if the username you requested is:
    - Already in use.
    - Very similar to an existing username (for example, if example@gmail.com already exists, you can't use examp1e@gmail.com).
    - The same as a username that someone used in the past and then deleted.
    - Reserved by Google to prevent spam or abuse.
- **Password**
  - Use at least 8 characters, consisting of upper and lowercase letters and numbers. Try using special characters such as ! and ? if you feel confident enough to do so.




## Username

Your username can be anything you want it to be, as long as it is available. You could use your name and some numbers, or maybe something different or random, like *trainspotter21* or *teacupdaisyflower99*

## Password

Use a strong password made up **UPPERCASE, lowercase, numbers and special characters.**

## Show password

Click the  to see the password you are typing. However, be sure no one is watching your screen if you do as they will see your password.

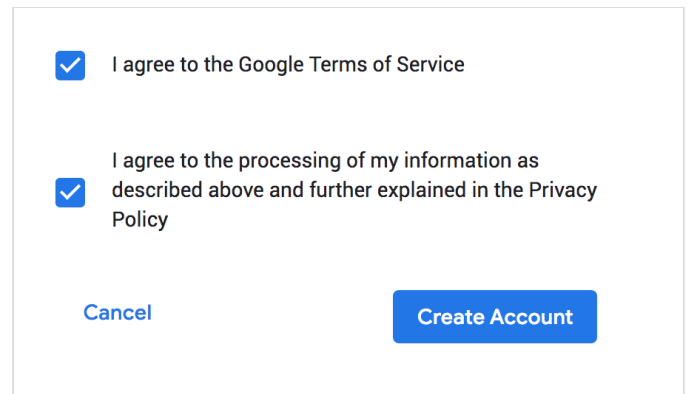
Click **Next** when you're done.

- The next screen will ask you for a little more information. Fill in as much as you are comfortable with, because this will help you should you forget your password and find you need to reset it.

Click **Next** when you're done.

- To be able to create your account you will need to agree to Google's Terms of Service. This is a long document that has a lot of standard items that the majority of web services use. A great website for seeing a summary of these in an easy to read format is:

**Terms of Service Didn't Read.org**  
(<https://tosdr.org/>).



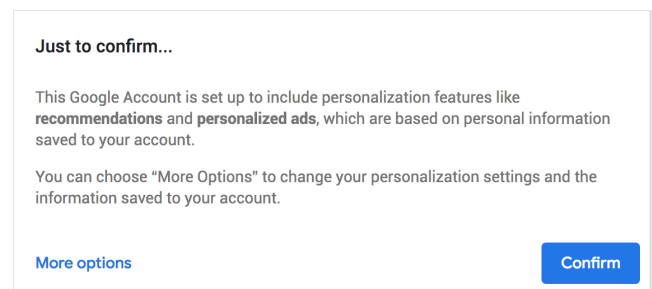
I agree to the Google Terms of Service

I agree to the processing of my information as described above and further explained in the Privacy Policy

[Cancel](#) [Create Account](#)

Click **Create Account**. You will then be prompted to confirm, notified that Google will personalise features using your information and browsing history. If you would like to change this then press **More options**.

Selecting **More options** will bring up another window, showing options for you to select.



**Just to confirm...**

This Google Account is set up to include personalization features like **recommendations** and **personalized ads**, which are based on personal information saved to your account.

You can choose "More Options" to change your personalization settings and the information saved to your account.

[More options](#) [Confirm](#)


An example is shown below, where you have the option on **Web and App activity**.

- Option 1: Allow Google to save your browsing history to your account, and therefore personal adverts and experience.
- Option 2: Don't save activity from web browsing or app use to your Google account.

**MORE OPTIONS** ^

Customize your Google experience by confirming your personalization settings and the data stored with your account.

You can always learn more about these options, adjust them, and review your activity in your Google Account ([account.google.com](https://account.google.com)).

 **Web & App Activity**

Saves your activity on Google sites and apps, including searches and associated info like location. Also saves activity from sites, apps, and devices that use Google services, including Chrome history. This helps Google provide better search results, suggestions, and personalization across Google services.

Save my Web & App Activity in my Google Account

Don't save my Web & App Activity in my Google Account

[Learn more](#)

It's up to you what you choose. Personally, we prefer not to save activity, as we do not wish to be targeted with adverts.

Once you have made your decision, click **Ok** and **Create Account**.

That's it, you've created a Google account and can begin to use features such as email.



## Password reminder

Use at least 8 characters, consisting of **upper** and **lowercase** letters and numbers. Try using **special characters** such as ! and ? if you feel confident enough to do so.



## Signing up to Google email (Gmail) on a tablet or smartphone

Although email can be accessed in a similar way on a smartphone or tablet, there is usually a specific app provided by the email service provider which allows for an easier and tailored experience.

### Download the app

There are many email apps available for download but the top two are provided by Google and Microsoft. If you are using a Google email account, then the best experience will be gained by using their Gmail App. Likewise, if you prefer to use Microsoft's services, then their Outlook App is the best option.

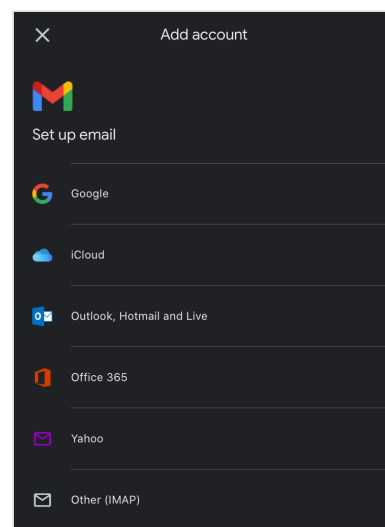
If you have more than one email account and with different providers, then you could use different apps for each, or use an app that supports multiple inboxes. In this guide we will be using Google's Gmail App as it does just this.

If you're not familiar with downloading apps, or even know what an app store is, then please refer to the below to our common tasks section, where we discuss this in more detail.

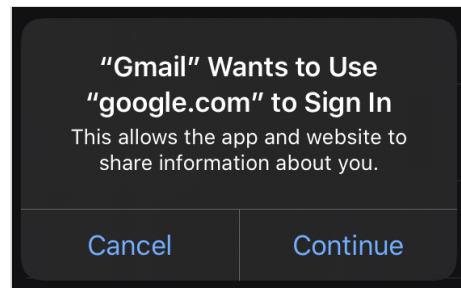
1. Once you've downloaded the Gmail App, tap **Sign in**



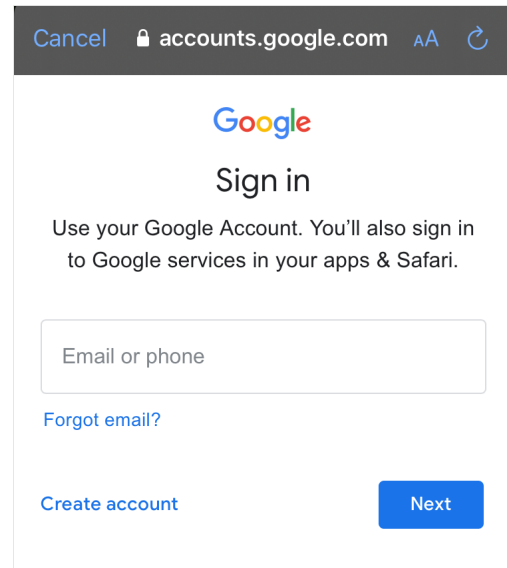
2. Now select the email service you wish to use. In this example, we are using Google.



3. You may be prompted with an additional question. If so click **Continue**.



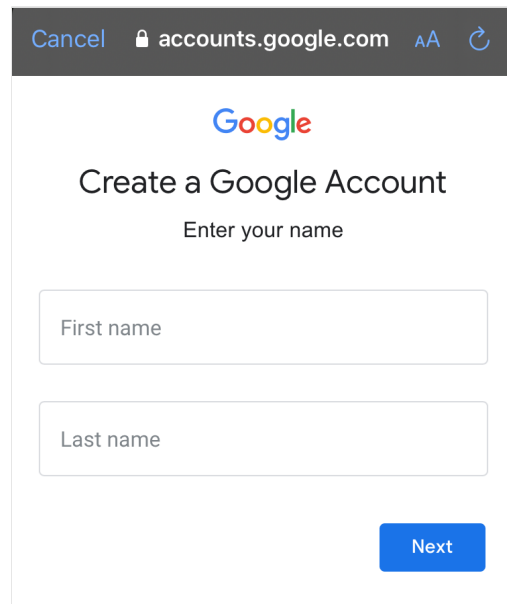
4. Now you have the option to sign in to an existing account, or choose **Create account** at the bottom of the screen.



5. On choosing **Create account** you will now be taken through a series of screens, asking core information to enable an account to be set up.

Information asked is:

- Name
- Date of Birth
- Email Address (what you'd like it to be)
- Password
- Phone number (optional and for account recovery purposes only)



Finally, you'll be asked a few options around privacy and security. It is nothing to worry about but read the sections and decide the options that best suit you.

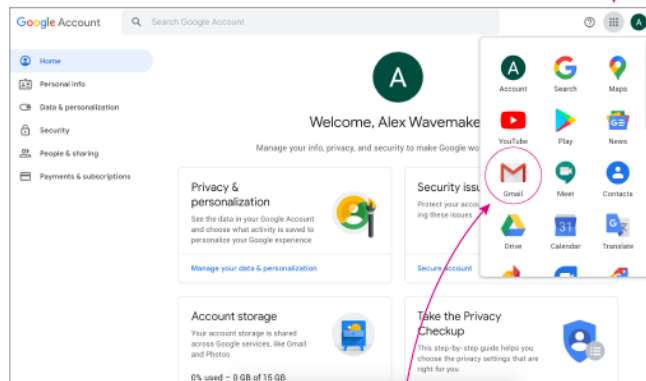


## How to send, reply and forward an email with Gmail on a desktop or laptop computer

### 1. Login to your Google account and open Gmail.

You can do this in a number of ways, like going to Google, clicking sign in and then using the navigation grid as shown in the image below, or by going directly to [mail.google.com](mailto:mail.google.com).

Whenever you log into Google on a web browser, you will use the navigation grid to find the app or service you are looking for.

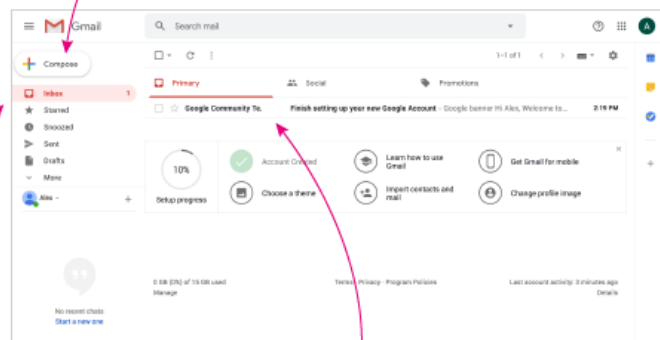


Your Google email logo looks like this, and is what you will need to click on to access your email.

### 2. Create a New Gmail Message

From the open Gmail inbox, click the **Compose** button in the upper left of the screen.

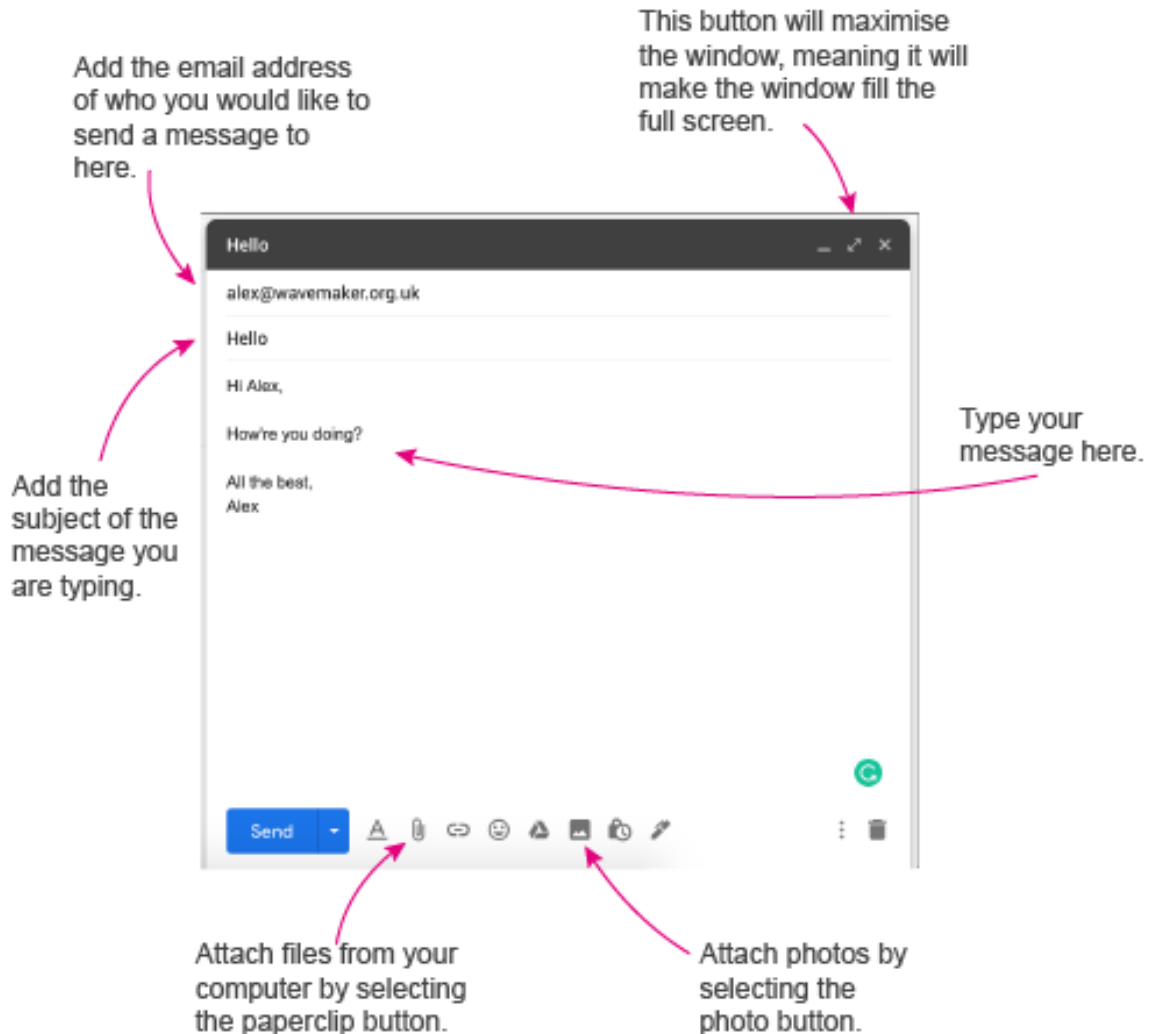
Start a new email by selecting the Compose button.



Messages can be viewed by selecting Inbox. All incoming messages go to your Inbox.

Messages are displayed here.

The New Message form displays.



Before you begin filling out the **New Message**, you can maximize it on your screen by clicking the **maximise** icon in the upper right corner of the screen (it looks like two diagonal arrows). This could make it easier to view.

On the New Message form there are three basic areas to fill out. These are:

- To field *(Who the message is being sent to)*
- Subject field *(A brief description of the message)*
- Body of the message *(Add your message, links, attach files and photos)*

There are also options that allow you to copy others on the message. Select the address bar to see:

- CC *(carbon copy)*
- BCC *(blind carbon copy).*  
This means the recipient cannot see who else you have sent it to.



### 3. Review Your Message

Before you send your new Gmail message you should review it carefully. Make sure that it says what you want it to say and that the information is correct. Gmail also provides a way for you to check spelling errors.

If your message is not quite complete you can save it as a draft. If you decide not to send the message you've created you can save it as a draft as well.

Select **Send** if you're happy and want to send the email.

### 4. How to Save as a Draft in Gmail

Messages are saved automatically, so you can just click on the **X** in the upper right corner of the New Message box.

Your message is saved in the Drafts folder and the New Message box closes.

### 5. How to **Delete** a message

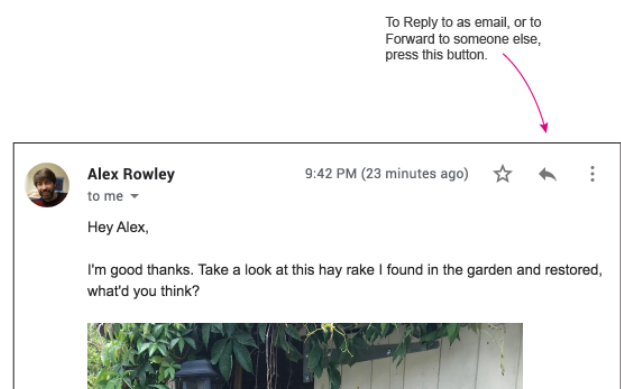
If you decide you do not want to send your new message, you can delete it. Click the delete button in the lower right-hand corner of the window. It looks like a rubbish bin.

## Replying to and forwarding a message

You can only forward a message that you have already sent or that you have received.

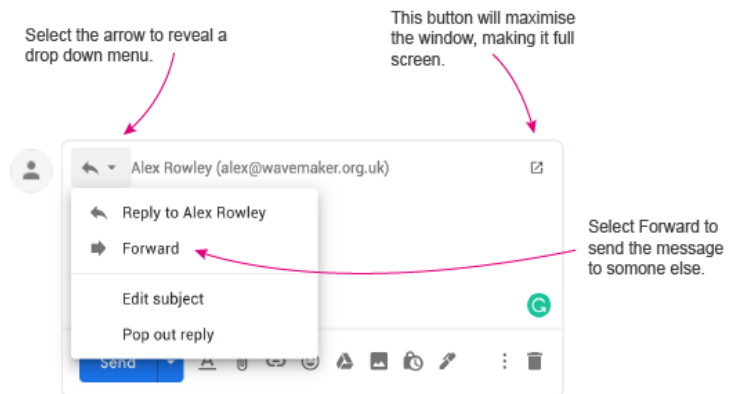
*You can find messages you have already sent in your Sent Mail folder.*

- Open the message you wish to forward and click the arrow in the upper right-hand corner of the message.



That will display the reply window. If you wish to reply, then type your message.

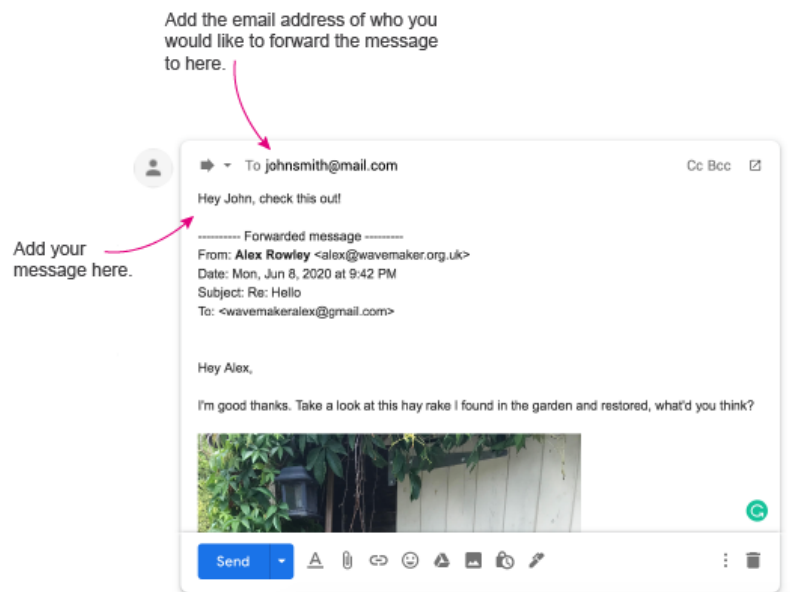
7. If you wish to forward the message to someone else, then select the arrow in the **upper left corner** of the window, and select **Forward**.



8. **Type the email address** of the person you wish to **forward** the message to in the **To** box.

Type any additional information you wish to include in the body of the text.

*Notice that Gmail adds a header to the original message that includes the email address of the original sender as well as the date and time it was sent.*



## Sending an email with Gmail app on a tablet or smartphone

Open the Gmail app on your smartphone or tablet and select **Compose**

A new window will now open, which is very similar to the one displayed when using a desktop or laptop computer.

The overview below covers all the core functionality to get you started.

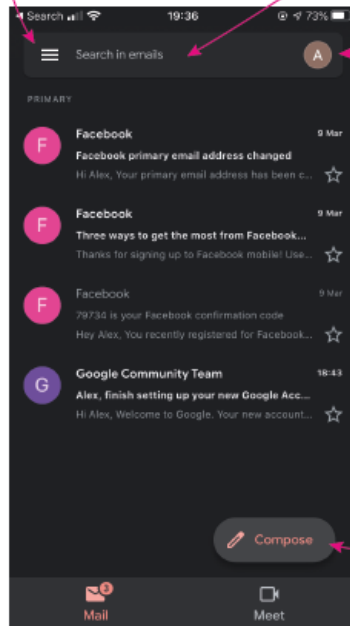
## Gmail app overview

### Menu bar

Use this to access different email folders such as sent, drafts and spam.

### Search bar

Use this to search your emails for keywords, topics or people.



### Account & settings

Here you can access your account information.

### Emails

This will display the relevant content for the menu being viewed, or search term entered.

### Compose

Use this to write a new email and send it to someone.

Emails

Video calling with Google Meet

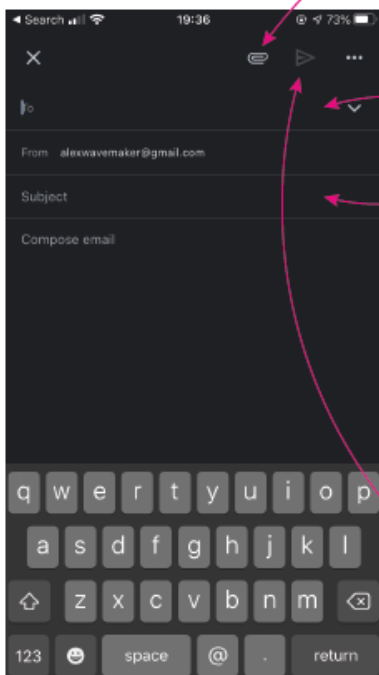
### Close

On tapping close you can choose if you want to save the email as a draft, or delete it.

### Attach files

Tap on the paperclip to attach and files or photos that you have on your device.

### Recipient



### Subject

## Sending emails

### Message box

Type your message in this box.

### Send

Tap the paper plane icon to send you email.

# Social media

Social media are websites that facilitate the creation or sharing of information, ideas, interests, and other forms of expression via virtual communities and networks.

Nowadays, there is a page, group or discussion for most businesses, organisations, places and topics.

There are many different social media sites offering different features that all cater to varying needs and interests, and as a result are preferred by various generations.

Here are the main ones, their uses and favoured age groups.

Service	Description	Typical age groups
Facebook	Facebook is the leading social platform, reaching 60.6% of internet users globally, that's 1.73 billion people.	45% of users are under 35 year old 35% are over 55 years old
Instagram	Instagram is the leading photo sharing social media platform, reaching one-billion users worldwide.	71% of users are under 35 years old  Most Instagram users are between 18-29 years old
Twitter	Twitter is the leading micro-blogging and social media platform, reaching 330 million users worldwide.	38% are 18 to 29 years old 26% are 30 to 49 years old 36% are over 50 years old

Joining and gaining access to a site such as Facebook allow you to engage in local groups and communities, as well as keep in touch with friends and family. We'll discuss facebook in more detail below.

## Facebook

Facebook is a social media website and service that allows you to connect with friends and the local community. It is especially good for keeping in touch with friends and loved ones, and for finding out what's going on in the local area. There are countless Facebook groups catering to a wide range of needs, whether local 'car boot' sales, history of the local area, or discussions around specific health conditions.



## Safety tip

Only accept friend requests from people who you know, or have met in real life. Always remember that anyone can set up a fake profile to impersonate someone else. Remain vigilant at all times.



## Signing up to Facebook on a desktop or laptop computer

Before you begin you'll need:

An email account

A mobile phone (for authentication)



1. Go to [www.facebook.com](http://www.facebook.com) to begin.

The screenshot shows the Facebook sign-up page. At the top, there are fields for 'Email or phone' and 'Password', with a 'Log In' button and a link for 'Forgotten account?'. Below this is the Facebook logo and the tagline 'Facebook helps you connect and share with the people in your life.' To the right, under 'Create an account', it says 'It's quick and easy.' and provides input fields for 'First name', 'Surname', 'Mobile number or email address', and 'New password'. There is also a 'Birthday' field with a date picker set to '9 Jun 2020' and a 'Gender' section with radio buttons for 'Female', 'Male', and 'Custom'. At the bottom, there is a 'Sign Up' button and a small disclaimer about terms and cookies.

2. Fill out the information under the **Create an account** section, adding your **name, email, or mobile number**, and **password, date of birth and gender**.

### Create an account

It's quick and easy.

Alex Wavemaker

wavemakeralex@gmail.com

wavemakeralex@gmail.com

.....

Birthday

4 May 1980

Gender

Female  Male  Custom

By clicking Sign Up, you agree to our Terms. Learn how we collect, use and share your data in our Data Policy and how we use cookies and similar technology in our Cookie Policy. You may receive SMS notifications from us and can opt out at any time.

[Sign Up](#)



### Safety tip

Ensure the password you choose is secure and memorable, but not the same password as your email account.

Once complete select **Sign Up**.

3. To finish creating your account, you need to confirm your **email** or **mobile phone number**. A code will be sent to your email, or phone via text message.

### Enter the code from your email

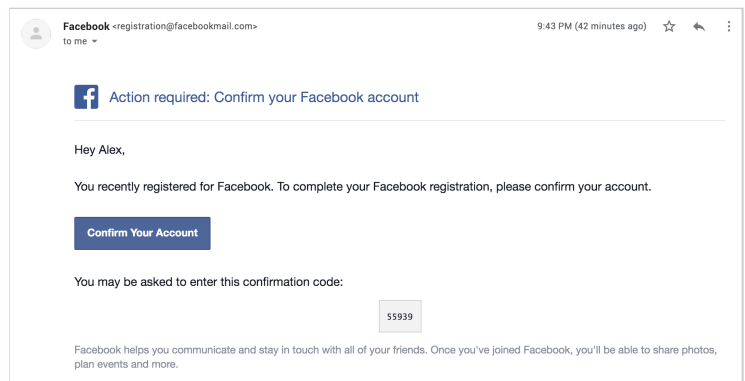
Let us know that this email address belongs to you. Enter the code from the email sent to **wavemakeralex@gmail.com**.

FB- 55939

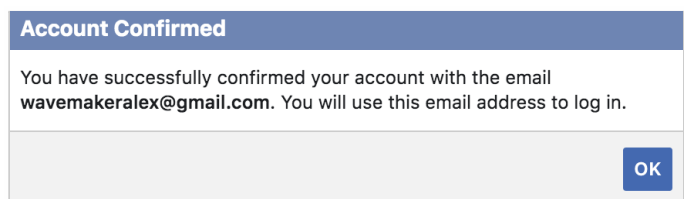
[Send Email Again](#)

[Update Contact Info](#)
[Continue](#)

4. Open your email or text messages to view the code sent by Facebook.



5. Once entered your account will be confirmed and you are ready to use Facebook.



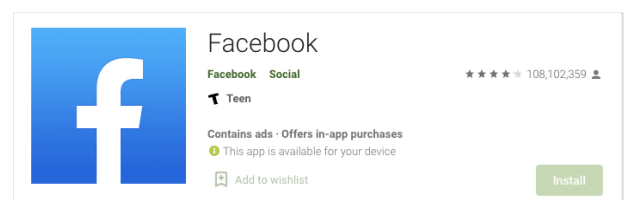
## Signing up to Facebook on a tablet or smartphone

Like email, Facebook can be accessed through an internet browser on a smartphone or tablet, there is a specific app provided by Facebook which allows for an easier and tailored experience.

### Download the app

Visit the app store on your device and search for **Facebook**, **select the app** and tap **Install**.

If you're not familiar with downloading apps, or even know what an app store is, then please refer to the below to our common tasks section, where we discuss this in more detail.







## Safety tip

Selecting the correct app is easy but always ensure you select the one created and published by Facebook. The publisher is displayed just below the name of the app.

1. Once you've downloaded the Gmail App, tap **Join Facebook** at the bottom of the screen.
2. You'll now be taken through a series of prompts asking you your name, date of birth and gender.
3. You now have a choice on whether to setup your account with your mobile number, or with using your email address.

### Join Facebook

We'll help you create an account in a few easy steps.

Get Started

### What's your name?

First name

Surname

Using your real name makes it easier for friends to recognise you.

### What's your mobile number?

GB ▼ +44 Enter your mobile number

You'll use this number when you log in and if you ever need to reset your password.

Use your Email Address

4. Create a strong password.  
Remember, **do not use the same password as your email account**, especially if you're using your email address to sign in.

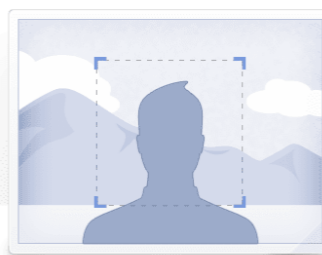
### Create a password

Enter a combination of at least six numbers, letters and punctuation marks (such as ! and &).

5. On finalising your account you'll be asked if you want to add a profile picture, and connect with others by searching your contacts to see who are on Facebook.

These can be done now or skipped until a later time.

Add a profile picture so friends can find you.



6. Finally, you'll be prompted to confirm either your phone number or email address, whichever one you used to sign up.

Let us know that this email address belongs to you. Enter the code from the email sent to [alexwavemaker@gmail.com](mailto:alexwavemaker@gmail.com)

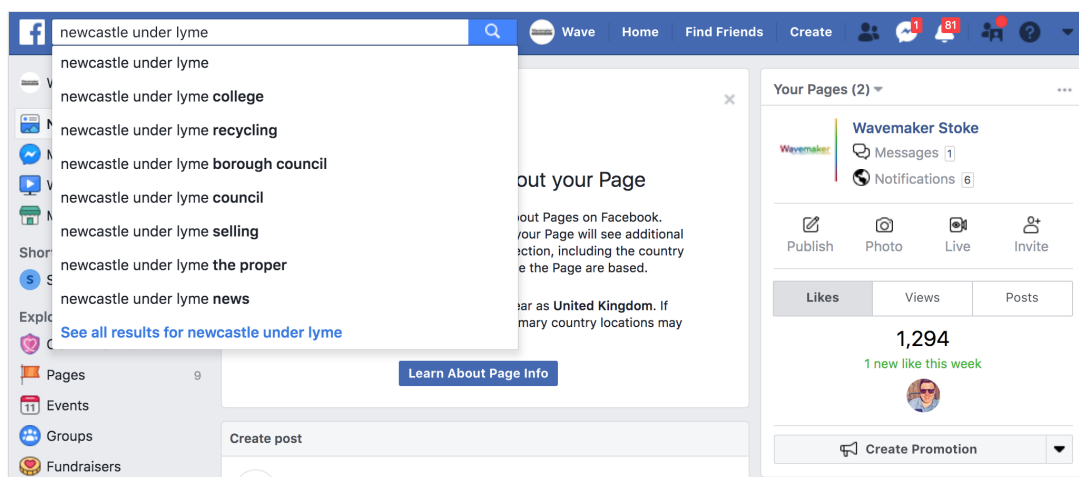


## Accessing Facebook groups and viewing pages on a desktop or laptop computer

Facebook has 2 billion users worldwide, and has a wide variety of information and support groups available at our fingertips.

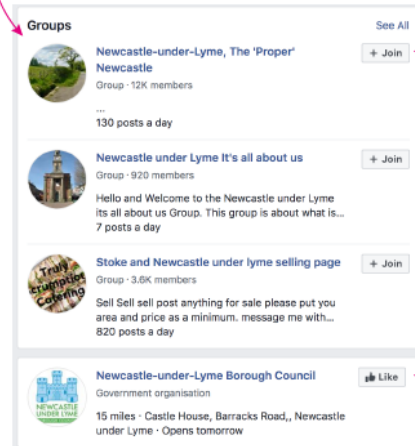
Facebook groups are particularly good for local information, whether it be news and events, history or sales. It is also extremely useful and popular for peer support groups for people managing particular health conditions.

1. Using the search bar will help you find what you are looking for.



2. Type in your search item, whether a person, a group or a local area and select search (press return/enter)

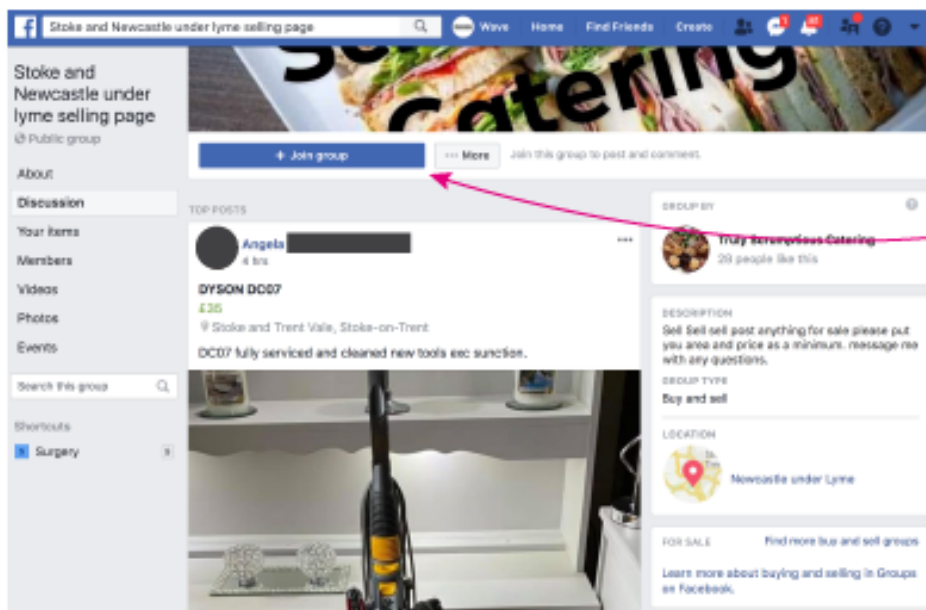
Search results are listed below. Select the one you want to view more information.



You can join from by selecting the Join button. However, we recommend viewing the group first to ensure it is the one you want.

Pages can't be Joined but they can be Liked.

3. Select the group or page to view, where you will be able to join, find out more information, and view posts.



This is the menu for the group, where you can find out additional information by clicking the links.

You can join from by selecting the Join button.

Item listings and other information is listed in the centre of the screen.

That's it! You're good to go and explore. Look for groups of interest, ones that help you improve your health, connect with the local area and enjoy yourself.

# Video Calling

Video calls can be made using a wide variety of equipment, as well as a wide variety of services. In this section we'll briefly note the most popular ones available, and give tips around video calling, but we won't go into detail for using each one as most are quite self explanatory.

## Equipment

Video calls can be made using technology that is now commonplace in many homes, such as:

- Internet enabled computer or laptop (with webcam)
- Smartphone
- Tablet
- Digital Assistant with screen (e.g. Amazon Echo Show / Facebook Portal)

## Software

There are many different services and apps to enable you to make and receive a video call, and depending on what device you use you will have different options open to you. Below is a table listing the common apps and services on what devices they are available on.

Video calling service / app	Device availability
<b>Apple Facetime</b>	iPhone, iPad, Mac Computers
<b>Whatsapp</b>	All Smartphones and Tablets
<b>Google Hangouts / Meet</b>	All Smartphones and Tablets, Computers and Laptops
<b>Zoom Meetings</b>	All Smartphones and Tablets, Computers and Laptops
<b>Microsoft Teams</b>	All Smartphones and Tablets, Computers and Laptops
<b>Facebook Messenger</b>	All Smartphones and Tablets, and Facebook Portal (voice controlled speaker and display screen)
<b>Alexa Video Call</b>	Amazon Echo Show devices, as well as all Smartphones and Tablets [with the Alexa App installed]

# Messaging Apps

There are many different messaging apps and services available to use. There is no reason why you cannot use more than one, and you'll find that each of the core ones have their own unique features and benefits. All the ones discussed here are free to download and use.

Service	Description
<b>WhatsApp</b>	Whatsapp is the most popular messaging app and owned by Facebook, It allows users to send <b>text messages, photos, voice and short video messages</b> to their WhatsApp contacts. They can also use it to make <b>voice and video calls</b> , and <b>join group conversions</b> .
<b>Facebook messenger</b>	Facebook messenger is an extension to your Facebook account, and can easily link you with anyone you interact with on Facebook to message or call.  It allows users to send <b>text messages, photos, voice and short video messages</b> to their WhatsApp contacts. They can also use it to make <b>voice and video calls</b> , and <b>join group conversions</b> .
<b>Signal</b>	Signal is a popular chat app and seen as an alternative to WhatsApp, as people migrate to this encrypted chat app in the wake of Facebook's plans to integrate Whatsapp into their platform.  It allows users to send <b>text messages, photos, voice and short video messages</b> to their WhatsApp contacts. They can also use it to make <b>voice and video calls</b> , and <b>join group conversions</b> .

## WhatsApp

WhatsApp is a messaging service owned by Facebook. It is free to use and has apps available to download on Apple and Android smartphones and tablets.

It's a free and easy to use messaging service that offers end to end encryption, and is therefore a safe and secure method of communication.

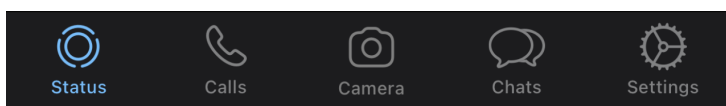
WhatsApp supports text messages, voice and video calls and group messaging.

To get started, download WhatsApp from the app store on your phone and open it up and follow the prompts to create an account.



## Overview of WhatsApp on a smartphone or tablet

Once you open the app, you will see the main controls and dashboard at the bottom of the screen.



### Status

**Status** is where you can add and update brief sentences to let your contacts know what you are up to. It could be something you're doing, or something about the mood you're in. You can also see any status updates of any of your contacts.

This is a feature more of an add-on and not best suited to WhatsApp core functionality - and something that is not used as much as the other features.



### Calls

**Calls** is the tab you choose if you're wanting to make a voice, video, or group call.



### Camera

**Camera** button is another way in which to update your status. You can add a photo or video which is made available for all of your contacts to see.

*Note: Do not use this feature if you are wishing to send a photo or video to a particular person or group of people, as this should be done from within the chats section.*



### Chats

**Chats** is where you can initiate and engage with text messages, both individual and group. Users have the ability to send and receive photos and videos. Voice and video calls can also be started from within chat conversations.



### Settings

**Settings** allows you to check and adjust any settings for Whatsapp. You can change items like your profile picture, what kind of background you'd like in your chat windows, and what type of notifications you receive.

## Groups

You can join WhatsApp groups or create your own. Groups can be a great way to share and receive messages and information. These could be between family members, local community groups, or support groups centred around particular topics or health conditions.



### Joining a WhatsApp group on a smartphone or tablet

There are a number of ways in which to join a WhatsApp group. Methods may differ depending on the group. You may get automatically added by the group admin (the person who set it up) or you may need to:

- Open a link that has been emailed or text to you.
- Open a link posted on a website, Scan a QR Code
- If you see a QR code on a poster or website, you can use your phone's camera to scan the link and join.

Almost all modern smartphones have QR capabilities built in, and can be accessed just by using the camera. In some instances, an additional app may be required.



# Jargon Buster

<b>3D Printing</b>	The practice of sending 3D computer generated models to 'print' as a physical object. Materials vary for printing ranging from plastics (for the printing of parts or jewellery) to research work into using organic materials for assisting certain medical procedures.
<b>3G</b>	Third generation mobile network technology enables access to the internet on tablets and smartphones (with an active mobile connection) This different to using Wi-Fi, and usually has contract costs.
<b>4G</b>	Fourth generation mobile technology is faster than 3G and widely available on newer devices. This makes surfing the web faster and accessing online services faster.
<b>5G</b>	The fifth generation (and latest) wireless technology offers speeds faster than 4G and is becoming closer to speeds achieved on home broadband connections. 5G is only available on the newest devices and in particular areas at the time of this guide.
<b>4K</b>	New high-definition screen resolution standard for TVs and computers (also known as ultra-high definition).
<b>A.I.</b>	AI (pronounced AYE-EYE) or <b>artificial intelligence</b> is the simulation of human intelligence processes by machines, especially computer systems.
<b>Android</b>	Google's operating system for tablets and smartphones; (android phones and tablets are an alternative to Apple iPhones and iPads).
<b>App (Application)</b>	Type of programme used on all smartphones, tablets and newer versions of Windows. They are installed onto your device through an app store, often low cost or free.
<b>Assistive technology</b>	Product or service that maintains or improves the ability of individuals with disabilities or impairments to communicate, learn, live independent, fulfilling and productive lives.
<b>Avatar</b>	A computer-generated character that can be used to simulate scenarios in healthcare for training and games (or serious games). Avatars can be programmed to respond in predictable ways based on human input in a virtual environment or can be operated by another human 'player' to speak via the virtual character and display virtual characteristics that may not be possible to show in a real-life role play. For example, the showing of injection marks, skin discoloration, abrasions or damage to skin or bone.
<b>Bluetooth</b>	Method for wirelessly connecting electronic devices.
<b>Blog</b>	A regularly updated section on a website or web page, typically one run by an individual or small group, that is written in an informal or conversational style.
<b>Bot</b>	A bot is a software program that operates on the Internet and performs repetitive tasks.
<b>Browser</b>	Computer programme that allows someone to use the internet
<b>Cloud</b>	The cloud refers to internet-based computing, where data or programmes are stored and accessed online rather than on a computer.

<b>Cloud print</b>	A wireless printing system used by Google tablets and smartphones that lets you print directly to compatible printers.
<b>Cloud storage</b>	Service that lets you back up and store your files online which is safer and more secure than storing them on your computer or on an external hard drive. You can access the files from anywhere on any compatible device via a smartphone, tablet or computer, by logging into your account. Cloud storage providers include Dropbox, Google Drive, OneDrive and iCloud Drive.
<b>Crowdsource</b>	Obtain (information or input into a particular task or project) by enlisting the services of a number of people, either paid or unpaid, typically via social media.
<b>Data</b>	Computer data is information processed or stored by a computer. This information may be in the form of text documents, images, audio clips, software programs, or other types of data.
<b>Device</b>	The item of hardware being used (e.g. smartphone, tablet or computer)
<b>Domain name</b>	A domain name provides an easy way of remembering an internet address. This name is unique. A domain name is your piece of internet real estate or your entry in a phone book.
<b>Dongle</b>	A device which is connected to an electronic tablet/laptop etc. that enables access to the internet.
<b>Encryption</b>	Encoding of data such that only those with the necessary authorisations can access it.
<b>Facebook</b>	Social media platform mostly used for a personal (non-work) profile and by professional organisations; you might set up an open or closed Facebook group.
<b>Firewall</b>	The security system on your computer that blocks access to certain website and online content that might harm your computer; and stop programmes on your computer from connecting to the internet if there is a potential safety issue.
<b>Gb (gigabit)</b>	This broadband is a high-speed type of internet, offering speeds of 1Gbps (Gigabit per second). Unusual for it to be for home based computing as it's expensive.
<b>GB (gigabyte)</b>	Measurement of data storage; a typical laptop will have 500GB or more of storage, while a tablet may have much less e.g. 16GB (a two-hour digital movie may be around 2GB in size; Word documents are smaller).
<b>Google</b>	Search engine to source information about (someone or something) on the internet.
<b>GPRS</b>	General Packet Radio Services (GPRS); a wireless communications service that allows access to the internet from an electronic device.
<b># (hashtag)</b>	A way for people to search for tweets that have a common topic and might also use to begin a conversation.
<b>Hits</b>	A hit is a request for one file from a web server. For example, if you request (i.e. visit) a single web page which contains only text, the web server will send you that page as a file. This process is called a 'hit'.
<b>Hotspot</b>	A physical device which allows people to connect and gain access to the internet.
<b>HTTP</b>	Hypertext Transfer Protocol (HTTP); the foundation of data communication for the World Wide Web.

<b>HTTPS</b>	Hypertext Transfer Protocol Secure. As above but with additional security protocols. All payment and financial websites should use this technology so look out for HTTPS when looking to purchase items online.
<b>In-App Purchase</b>	In-app purchases are extra content or subscriptions that can be bought from inside an app. Not all apps offer in-app purchases.
<b>Instagram</b>	Online mobile photo-sharing, video-sharing, and social networking service that enables users to take pictures and videos, and share them either publicly or privately on the app, as well as through a variety of other social networking platforms, such as Facebook, Twitter, Tumblr and Flickr.
<b>Interactive</b>	Two-way transfer of information between a user and the central point of a communication system, such as a computer or television.
<b>Internet of Things (IoT)</b>	The practice of connecting everyday devices to the internet so they can send data regarding their usage or other measurements over time.
<b>iOS</b>	Apple's mobile operating system, used on the iPhone, iPad and iPod Touch, but not on iMacs or MacBooks.
<b>IP Address</b>	Internet Protocol (IP) address. A unique combination of numbers that is used to identify each electronic device which is communicating over a network that utilises IP (i.e. a set of rules that dictates the type of data sent over a network).
<b>iPhone</b>	Smartphone made by Apple that combines an iPod, a tablet PC, a digital camera and cellular phone. The device includes internet browsing and networking capabilities.
<b>ISP</b>	Internet service provider (ISP); a company that provides access to the internet and other web-based services.
<b>LinkedIn</b>	A social media platform designed and used as a professional network.
<b>MB (megabyte)</b>	A measure of data storage; a large digital picture file might be around 2MB in size for instance.
<b>Mbps</b>	Megabits per second is the term used to measure broadband internet speeds; the national average speed is around 2Mbps, but high-speed services can be over 30Mbps.
<b>Meta</b>	Meta, formerly known as Facebook Inc, is an American multinational technology conglomerate based in California, and the parent organisation of <b>Facebook</b> , <b>Instagram</b> , and <b>WhatsApp</b> , among other subsidiaries.
<b>MIFI</b>	Mobile wifi device used to connect phones, tablets and computers to the internet
<b>Mp (Megapixel)</b>	One million pixels; a measure of the size of digital photos. The more megapixels, the higher the resolution and level of detail.
<b>Multimedia</b>	Content that uses a combination of different content forms such as text, audio, images, animations, video and interactive content.
<b>Network</b>	A group of electronic devices connected together that allow data sharing.
<b>Notification</b>	An alert or banner from a particular app on your device.
<b>Office 365</b>	A subscription version of Microsoft's Office suite, for which you'd pay an annual fee of around £60 for access to Word, Excel and other programmes.

<b>OS</b>	An operating system (OS) is system software that manages computer hardware, software resources, and provides common services for computer programs.
<b>Phishing</b>	An online scam that tricks someone into giving away personal details using a fake website or e-mail that appears to relate to an authentic service.
<b>Router</b>	Device that sends data from one network to another.
<b>SD card</b>	Small memory card typically used in digital cameras and some laptops. Newer versions are termed SDHC and SDXC, with higher storage sizes.
<b>Sensor</b>	Device that responds to a physical stimulus (as heat, light, sound, pressure, magnetism or particular motion) and transmits a resulting impulse (as for measurement or operating a control).
<b>Skype</b>	Application for communicating with other people over the internet using video interaction or voice calls.
<b>SIM</b>	Smart card inside a mobile phone, carrying an identification number unique to the owner, storing personal data, and preventing its operation if removed.
<b>Snapchat</b>	Mobile app that allows users to send and receive 'self-destructing' photos and videos. Photos and videos taken with the app are called snaps.
<b>SSL Certificate</b>	An SSL certificate is a digital certificate that authenticates a website's identity and enables an encrypted connection. SSL stands for <b>Secure Sockets Layer</b>
<b>Syncing</b>	File synchronisation between two locations (between two different devices or within the same device).
<b>TECS</b>	Technology enabled care services are any care approaches which utilise a form of technology for delivery of health or social care.
<b>Telecare</b>	Remote care of elderly and physically less able people, providing the care and reassurance needed to allow them to remain living independently in their own homes (sometimes used interchangeably with the term 'assistive technology').
<b>Telehealth</b>	Means or methods for enhancing delivery and support of health care, public health and health education using telecommunications interactive or information mobile texting or phone lines.
<b>Telemedicine</b>	Video consultation by health care professionals allowing them to evaluate, diagnose and treat patients in remote locations using telecommunications technology.
<b>Tethering</b>	Circumstances when an electronic device is designated as a mobile hotspot so that other devices can wirelessly connect and use the internet via the device's internet connection.
<b>Texting</b>	Act of composing and sending electronic messages between two or more users of mobile phones or portable devices e.g. tablet, computer or smartphone.
<b>Twitter</b>	Social media platform where time sensitive news, views and opinions can be shared.
<b>URL</b>	A Uniform Resource Locator (URL) is another term for a web address.
<b>USB</b>	Universal Serial Bus (USB) is a very common type of computer connection; USB ports are used to connect PCs with other devices, such as printer, computer mouse and external hard drive. The fastest version is termed USB 3.0, also known as SuperSpeed USB.

<b>Video consultation</b>	Provision of consultation services by health professionals to patients who are sited in different locations (similar to term 'telemedicine').
<b>Vishing</b>	Vishing is the telephone version of phishing. Instead of e-mail messages with suspicious links or attachments, criminals attempt to fool you into giving them the same information in a phone call. Vishing uses techniques to trick you into providing information that can be used to access and use your financial accounts. For example, the fraudster may claim to be an employee of your bank who wants to warn you of some suspect charges on your credit card.
<b>VR</b>	<b>Virtual reality (VR)</b> is a <u>computer-generated</u> scenario that simulates experience. The immersive environment can be similar to the real world or it can be fantastical, creating an experience not possible in our physical reality such as walking through imaginary planets. To experience VR the user will need to wear a headset with lenses and it is usually attached to a smartphone which shows the film through a VR app.
<b>WhatsApp</b>	An instant messaging social media platform owned by Meta.
<b>Web browser</b>	This displays a web page on a monitor or mobile device.
<b>Webmail</b>	Type of email service where messages are stored online in the cloud, rather than saved as files to a computer. Access is from any PC, tablet or smartphone by secure log in. Outlook.com, Gmail and Yahoo! Mail are all free webmail services.
<b>Web pages</b>	Document that is suitable for loading on the World Wide Web and web browsers.
<b>Web server</b>	Computer system that processes requests via HTTP, the basic network protocol used to distribute information on the World Wide Web.
<b>Website</b>	Collection of related web pages including multimedia content, typically identified with a common domain name and published on at least one web server.
<b>Wi-Fi</b>	Wireless service that allows electronic devices to connect to the internet.

# Password Passport

With so many sites and services that we have to sign up for, it is easy to forget what's what. Even though you may use techniques to remember different ones, it is sometimes useful to write them down. **Please note that if you do then you must keep this booklet extremely safe and secure, as its loss could leave your accounts vulnerable.** As an additional tip. We do not recommend you write your full password in, and should omit certain parts only writing what you need to remember.

This could be the beginning, the middle or the end, but not all of it - so to safeguard being guessed should this book be misplaced.

For example, if your password was **TreeTop35!** then you could write **T\*\*\*\*\*3\*!**

Service / Site	Username	Password
<i>E.g - Google Mail</i>	<i>wavemakeralex@gmail.com</i>	<i>T*****3*!</i>





