Digital World Library

Have you come across a new word?

Here you can find out what words like ‘Algorithm’, ‘Fake News’ and ‘Cyberbullying’ mean.

You can also find out about new online features and tools such as ‘Live Streaming’

Look out for some additional library CHALLENGES, helping you learn even more about the digital world!

Algorithms

For a computer to be able to do anything, it needs instructions. In simple terms, an algorithm is a bit like a recipe with a sequence of instructions for your computer to follow and carry out tasks.

Social networking site Facebook uses algorithms for many reasons, including:

- Selecting which posts will show up on your news feed.
- Recommending contacts that you may be interested in.
- Suggesting pages based on your likes.
- Detecting harmful links that may be spam or viruses.
- Showing you adverts that are relevant to your interests.

Anonymity

This is a feature that some apps allow. People may make an account posing as anybody they want or use an anonymous messaging app to send comments to other users without ever knowing who they really are or where they came from. Some apps are also designed so that you can't reply to the messages.

What are the risks?

Being anonymous makes it easier to be unkind to others. It enables some people to pretend to be someone else; this is known as *catfishing*. Before joining a service that allows anonymity, be sure you know how to report and block users who could potentially be unkind or harmful.

Applications – 'Apps'

An application is more commonly referred to as an app. These can be any type of computer program.

Apps are usually downloaded onto smartphones or tablets. You can usually access an app by clicking on the small icon/image on the smartphone or tablet device. Some apps are free and usually already on devices such as the calendar or calculator apps. Others must be purchased and downloaded. Many companies have their services available in app form to make it easier for customers to access, such as online banking apps and online shopping apps.

Many young people use chat and social media service such as WhatsApp, WECHAT, Instagram and Facebook through apps on their smartphones.

Blocking

Apps and websites that involve interaction with other people, including online gaming platforms and social media sites, allow you to stop other people from communicating with you and stop them from seeing your posts and information. This is called blocking.

The ability to block people can help keep you safer and more comfortable when exploring the online world.

Here are some reasons you may decide to block someone online:

- You are being cyberbullied or trolled online.
- You receive spam messages from fake accounts and *bots* (computer-generated messages).
- Someone is being unkind to you in an online gaming platform.
- You receive inappropriate messages from someone you don’t know.

You need to check individual websites for instructions on how to block someone and what they can and can’t see once they’re blocked. You may worry that the person you block will get a notification telling them that they have been blocked. Don’t worry, this doesn’t usually happen. But, it is best to check the information on the website because each service provider has its own blocking process.

CHALLENGE*: Choose a popular website and research its blocking process. Write it down in simple terms and see if you can describe to someone else how you might block someone online.*

Blog

This is a regularly updated website or web page, typically run by an individual or small group. It is usually written in an informal or conversational style.

Anyone can set up their own blog and it is quite simple to do. It can be a fun way of writing about your interests or hobbies. Some people set up blogs to support other people who may be going through the same problems as them. This is called peer-to-peer support.

Be aware that not all blogs are reliable. Some people may express their opinions, without evidence to back up their views. Some blogs may contain extreme, disturbing or harmful opinions and images. Read up on fake news to see how to spot reliable information.

Browser

A web browser is a software application for accessing information on the World Wide Web.

Some of the most popular browsers are Chrome, Safari, Firefox and Microsoft Edge (replacing Internet Explorer as the default web browser). You can open a browser to search for web pages, images, videos and other information resources online.

Catfishing

In the digital world, a *catfish* is someone who pretends to be someone that they're not.

For example, it is easy to set up a fake social media profile, make up a name, upload a photo of someone else and pretend to be them. Sometimes people use this so that they can spread hateful and harmful messages online whilst staying anonymous.

If someone you don't know tries to add you as a friend online, or sends messages, be wary that the name and photo they are using may not really be their real one.

Sometimes a *catfish* will try to trick others by uploading what they consider to be attractive photos to get people to accept their friend request.

Cyberbullying

Cyberbullying is online bullying. If someone is repeatedly unkind or harasses another person online, then they are a *cyberbully*.

Cyberbullying is slightly different to online trolling, although the two words are often, and can be, used interchangeably.

Cyberbullying usually involves people you know. It is often accompanied by traditional, offline, bullying.

Whereas trolling can include comments and messages to people you have never met, to provoke them or start an argument.

Top tips to remember:

- Always report cyberbullying to a trusted adult, even if it isn't happening to you. Report it on behalf of a friend who may be too scared or upset.
- Ask an adult to help you block and report the cyberbully online.
- Never respond to a cyberbully with messages. Just report it and seek help.
- Although you may want to delete nasty messages, make sure you collect evidence to show a trusted adult.

Digital footprint

Your digital footprint is the mark that you leave behind when using the internet. It can shape your online reputation.

Your digital footprint includes all the content you create, post and share; as well as any content that others post, and share, with you and about you. To have a positive digital footprint it is important to think carefully about what you are sharing, liking and posting online.

Make sure you are not leaving behind anything negative that may affect your online reputation. For example, if you search your name and silly or inappropriate photos of you appear, that have been shared in public, then chances are your teachers, or any future employers, will be able to see them too.

***CHALLENGE**: Try cleaning up your own digital footprint. Search for yourself online and delete anything that you think may be harmful, embarrassing or just a case of oversharing. You could practise changing your privacy settings so that all your information is protected and that you know what people can see, if they were to search for you online.*

Digital resilience

The UK Council for Child Internet Safety (UKCCIS) Resilience Working Group’s definition of digital resilience is:

‘…the ability to understand when you are at risk online, knowing what to do if anything goes wrong, learning from your experiences of being online, and being able to recover from any difficulties or upsets.’

A person who is digitally resilient will be able to:

- Understand when they are at risk online.
- Know what to do to seek help.
- Learn from their experiences.
- Recover when things go wrong.

Encryption

Encryption is the process of converting information or data into a code, especially to prevent unauthorised access. End-to-end encrypted messages can only be read by the sender and the receiver. This can be both good and bad.

The good thing is that when a message is encrypted it is more secure and private. This is useful for important and sensitive information.

The bad thing is that some people may take advantage of this and use the end-to-end encryption to spread harmful information that cannot be moderated and tracked.

Exploitation

There are people online who may take advantage of vulnerable people and exploit them to get something from them that they want. If this happens to a young person, it can make them feel upset and ashamed. They may feel like they are to blame, even though it isn’t their fault.

It is important to let a trusted adult know if anything happens online that makes you feel ashamed. Even if it is not easy to say, you need to find someone you trust who can help you report it and recover from it.

Facebook

Facebook is the biggest social media network in the world with over two billion users across the globe.

On Facebook you can:

- Make a profile.
- Upload photos.
- Update your status.
- Add friends.
- Join groups.
- ‘Like’ photos and statuses.
- Live stream using Facebook Live.

Facebook aims to have as many users as possible and the easiest way of achieving this is by ensuring that they provide people with a free service.

Facebook makes money by selling advertisers your information. This includes details about your Facebook ‘likes’, interests and any links that you click on. For example, if you always ‘like’ and share information about sports, you may notice that Facebook will display adverts that relate to that interest.

Advertisers will then know which adverts are best to show on your page and this gives them a more targeted advertising approach.

CHALLENGE*: Next time you go on the internet, look out for any adverts that appear on your page. Make a note of the different products and services being advertised and see if they appear to match your own personal interests. Do you think the adverts are targeted?*

Fake news

You may have heard of the term ‘fake news’ talked about in the media or between friends. There are different types of fake news.

Some fake news is deliberately made up stories or images with the aim of making people believe something that isn’t true.

Others have some truth to them, but may be misleading, including some false information that hasn’t been checked properly or with facts that have been exaggerated by the author.

Spotting whether something is fake news is not always easy. With so much information produced online, and the speed that information is posted and spread, even reputable news sites have been caught out accidentally sharing unreliable stories. Of course, they take them down from their websites or social media accounts as soon as they realise, but this is usually after the stories have already been seen and shared across the world.

Although it is not always certain, there are some ways to help you work out what is most likely to be reliable online and what may not be:

- Has the story been repeated elsewhere? Check other reputable sites.
- Does the image look believable? Is it used elsewhere? For example, an edited photo of a pink giraffe flying across the moon is a big clue that the story isn’t real!
- Does the web address (URL) look strange? Or is it from a trusted site?
- Do you know who the author is? Have you heard of the organisation reporting it?
- Are you familiar with the organisation or company? Are they reputable?

CHALLENGE*: Find an example of something unreliable online. Show it to an adult and talk them through how you can spot why it is unreliable. Discuss the difference between something that is unreliable and something that is harmful or unsafe.*

Hacker

A hacker is someone who manages to gain unauthorised access to some data. This means that they didn’t have permission to access it. This could be someone accessing an online social media account or even managing to hack a company website or access confidential documents and data.

Hackers will often use phishing scams to get the information they need to access an account or website without the owner’s permission.

Hate speech

Hate speech is speech which attacks a person or group based on attributes such as race, religion, ethnic origin, sexual orientation, disability, or gender. It is important to be wary of posts online that may be examples of hate speech and avoid liking and sharing offensive information. Often a post online is mistaken as a harmless joke and may be shared on social media, but it is important to think about the consequences of spreading information from organisations that incite hatred and in some cases violence against certain groups.

Instagram

Instagram is a very popular photo sharing app and service that allows you to upload photos and videos to share them either with friends or anyone by making your profile public. On Instagram you can:

- Upload photos or videos of yourself.
- ‘Like’ other people’s photos by tapping the heart button.
- Comment on photos.
- Use hashtags to make your photo popular.
- Build up followers and get followed back.
- Use ‘Insta DMs’ to message your followers privately.
- Use live streaming though Instagram Live!
- Add photos and videos to your Instagram story. This is similar to Snapchat.

#ad #sponsored

Sometimes celebrities are sent new products and paid to show them off to their many followers on Instagram. This is a type of advertising and it should be made clear in the description or hashtag that the person is being paid to promote something. It may not be a true reflection of their opinion.

Kik Messenger

Kik is a free messenger app where users can send messages, images and even sketches to each other. There are no word or character limits and no fees for this app.

One of the main risks is that users can randomly connect with strangers and have conversations. Although users are free to leave the conversation at any point, some people have questioned how safe it is for younger children. It is worth being aware of this if you're using the app.

There are no in-app purchases, but the Kik Code function encourages users to use Kik to connect to commercial brands and point them towards other sites. Kik uses these QR codes to gather information about the user.

Live Streaming

Live streaming is the broadcasting of real-time, live, video to an audience over the internet. All you need is an internet-enabled device, such as a smartphone or tablet, and a platform to broadcast on.

Why are live streaming platforms so popular?

Live streaming is highly appealing as it presents the chance to be a creator, a presenter and to be seen by a potentially huge audience. You can broadcast anything you are doing across the world without delay.

Some apps that allow live streaming:

- Facebook
- Twitter
- Instagram
- ly
- Me
- YouNow

What are the risks?

Being able to broadcast yourself online can be fun and exciting as it lets you be the star of your own show, but it is important to know that there are some risks to being so visible online:

- You never know who's watching – if your live stream is popular with loads of viewers it might be promoted so people who don't follow you can tune in too if your profile is public.
- You never know what you're going to see – when watching someone else's live stream you can never tell what's about to happen. This can be part of the fun of live streaming. But, you might be exposed to harmful or upsetting content by other users.
- Not all viewers are friendly – viewers can comment on your live stream as it happens, and their comments might be mean, rude or inappropriate and can make you feel sad or scared.

- Letting people know where you are – you should be mindful of what you're revealing in your live stream. If you're in your school uniform or close to your house you could be letting strangers know where you go to school and where you live, even if you don't verbally say it.

CHALLENGE*: Have a debate with a friend or family member about the positive and negative aspects of live streaming.*

Moderation

For an online space to be considered safer it needs to be moderated. This means the content of the website or app is overseen by someone called a *moderator*. A moderator's job is to make sure that nothing irrelevant, abusive, harmful or illegal is contributed to the website.

Here are some common online spaces that are moderated:

- Forums
- Blogs
- Social media sites (Facebook/Twitter etc.)
- Online groups

How does it work?

In most cases a moderator will regularly check the website or app to make sure everyone is adhering to the set rules and regulations. In some cases, comments or posts will be flagged and reported by other users who deem it offensive, harmful or breaking the rules of the site.

The moderator will then review the case, and if it has broken the rules then the post will be removed. The person who posted it will be alerted that their post has been removed. If they are a repeat offender, then they can be permanently blocked from posting again.

How does moderation make a website or app safer?

A website or app that is regularly moderated is more likely to have a positive and encouraging atmosphere. It helps make sure that those who do not want to abide by the rules are dealt with.

However, there are lots of people who go online every minute of the day from all over the world and moderating websites is a tough job. Many social media companies are under pressure, and have promised, to employ more moderators to help make their sites safer. As the number of internet users continues to grow it is going to get harder to keep up.

Some social media sites can be unmoderated, which means there isn't someone overseeing what's happening between users. Some messages are encrypted meaning others can’t read them. If no one is checking to ensure everyone is safe and secure; anything can happen.

***CHALLENGE**: Next time you go on a popular website or app see if you can find information about moderation or moderators. Do you think they are doing a good job? How could they improve? Discuss with a friend or family member.*

Netiquette

If you merge the words internet and etiquette together you get the word netiquette. This refers to how to behave online. Following the rules of netiquette involves exploring the digital world in a way that is positive for both yourself and others you may encounter along the way.

You may notice that netiquette overlaps with online empathy, that is because being empathetic and kind to others online is a big part of following the rules of netiquette.

It can be hard to read other people’s emotions when chatting online and this makes it easy to misunderstand others. Have you ever sent your friend a message that was meant as a joke, but they didn’t understand whether you were being serious?

There are people that don’t follow netiquette and deliberately send out hateful, negative messages by ‘trolling’ others, posting abusive comments on social media or spreading fake news. It is best not to respond or engage with these people. Tell a trusted adult about what happened so they can support you and report and block the user.

Here are some simple rules of netiquette that can help make your experience online safer and more enjoyable.

- Check before sharing images or videos of your friends or other people. They may find them embarrassing or simply not want them to be made public. It is also important to bear in mind that photos and videos of other people is their personal data, so you should get permission before sharing.
- Think before you post anything. Is it going to upset, embarrass or offend anyone? This includes writing nasty comments on a celebrity’s social media post. Trolling people that you don’t know is still unkind!
- Check if information is true and reliable to the best of your knowledge before accidentally spreading what could be misleading information.
- Think carefully about how you may come across in emails, messages or comments. For example, writing in capital letters to your teacher may come across as rude or even aggressive, even if you don’t intend it to.

***CHALLENGE**: Think about what you usually do online and decide whether you usually follow the rules of netiquette. If not, what could you change? Discuss with a friend or family member.*

Online empathy

Empathy is an emotion that allows you to be aware of your impact on other people and understand how they might feel in response to something you say or do.

For example, someone may be going through a tough time and feel as though lots of bad things have happened. If you're able to understand why this makes them feel so bad, then you're being empathetic. You're showing empathy.

Being empathetic is different to being sympathetic. Empathy is about being able to put yourself in their shoes, whereas sympathy is about expressing the fact that you care about what has happened, rather than understanding someone's feelings.

Being empathetic is particularly important online when interacting with others on apps such as Snapchat and Instagram or talking to online friends when playing games, or on websites or messaging apps. It is important to put yourself in other people's shoes and think carefully before doing or saying certain things online.

How can you practise online empathy?

- Think before you post a comment or message, especially if it is about someone else. Would you say it to them in person? How would you feel if someone said the same about you?
- Think before you share a video or photo online. Will it upset, anger, embarrass or offend anyone? Is it appropriate? Are you aware how many people will be able to see and share it?
- Be nice. What you say can have a negative impact on someone and how they feel. It can even impact their mental health.
- Don't engage if you see someone being cyberbullied. Tell a trusted adult and report the abuse, but don't interact with the bully or bullies.
- If someone asks you to remove a photo of them that you've posted, take it down. Understand how you would feel if someone had done the same to you.
- Be kind to yourself too! Remember that not everyone's life is as exciting or 'perfect' as it may appear to be on social media. If scrolling through other people's photos and videos just makes you sad or envious, take a break. Bear in mind that people choose what to show about themselves, and their lives, and can add filters and edits to images to change them.

CHALLENGE*: Think of one thing that you can do next time you're online that shows online kindness or empathy. It could be as small as sending a positive message to a friend to cheer them up or make them laugh.*

Online reputation

Your online reputation is what anyone can find out about you if they were to search for you online. This could include photos that you have made public, posts that you have shared on social media for everyone to see or photos and videos with you in them, shared by others.

It is worth thinking about your online reputation and the digital footprint that you have left behind.

Of course, it is hard to control what others say and share about you online. But, you can think carefully about what you're making public.

Before you make a public post, consider how you would feel if a parent or teacher saw it. Are you happy for it to be seen by anyone in the world?

Passwords

A password is a secret word, phrase or combination of characters that allows you access to protected information or an account.

A strong password is one that is secure and not easy to guess. It can be used to help protect your information online, keeping it private.

Here are some handy tips:

- Create different passwords for different accounts.
- Choose a password that is not easy to guess.
- Use a mixture of numbers, characters and lower and upper-case letters.
- Avoid obvious words such as your own name or your pet's name.
- Avoid obvious numbers such as your date of birth, age or phone number.
- Instead of just one word, think of a short phrase that nobody would guess.
- Keep your passwords secret, even from your best friend!

CHALLENGE: *After you have read the tips above see if you can come up with some strong passwords. Now is a good time to change any passwords for online accounts, making sure you keep them all to yourself.*

Peer-to-peer

Peer-to-peer support is when people use their own experiences to help others and themselves. It is support based on shared experiences. People who have experienced similar challenges can offer insight into how you may be feeling and offer strategies that worked for them.

An example of this would be someone living with a condition, such as epilepsy, who decides to write a blog to share with others and help them. They may make a daily *vlog* (video blog) about how they are living with epilepsy. They may reply to comments from other people online and indicate where to get support and share advice and tips about things that help them feel better.

What are the risks?

The great thing about the internet is that young people can self-generate their own content and share it with their friends and others. However, it is difficult to moderate self-generated content such as blogs or vlogs. Some information in them may be misleading, harmful or factually incorrect.

Not everything you see and read online is true. Peer-to-peer content can sometimes be fantastic and provide much needed support for dedicated followers. However, it can come from a biased point of view, designed to encourage people to think a certain way or even cause harm.

It is crucial to develop *critical thinking skills* when dealing with information online. This means asking yourself if you think what you're reading is true or not. Does it sound realistic? Can it potentially be dangerous? This goes for anything you see online, whether it is written content, online rumours or a photo that has gone viral.

***CHALLENGE**: Make a list of the positive and negative aspects of peer-to-peer support and explain them to someone else.*

Personal information

There are different types of personal information or personal data. This is information about yourself that it can be risky to share online in a public place. This is because strangers may also be able to see this information. Examples include:

- Home address.
- Telephone number.
- Email address
- The name of your (child's) school.
- Full name and date of birth.

Other information may also be personal, but not considered risky to share. For example:

- The fact that you love sports.
- Your pet dog's favourite food to snack on.
- Your favourite book or film.

When you go online it is important to consider which kind of information you need to keep private so that strangers online can't find out too much information about you. It is also important to bear in mind that a photo of a friend or other personal information about a friend is considered their personal data. Therefore, it is important to check with a friend before sharing a photo of them or tagging them in it.

Phishing

Phishing is when scammers attempt to trick you into giving out personal information such as your bank account numbers, passwords and credit card numbers. It could be presented as an email asking you to give your credit card details to confirm a purchase that you never made, or a popup saying that you have won a new smartphone, requesting your personal information to claim your prize.

Some phishing scams can be quite realistic. Scammers will often pretend they are writing on behalf of real companies, that you may have an account with. It is important to check emails and messages carefully.

Here are some tips to help you work out if something is a phishing scam:

- No reliable company will ask you to give away your password.
- If you did not apply for a competition and you see a popup saying you've won a prize, then it is most likely a scam.
- Check the sender's email address very carefully. Even if they pretend to be from a real company that you have an account with, scammers have strange email addresses full of numbers and characters that won't match the official company address.
- Search for official email addresses online to double check.
- Report any phishing emails to your email service provider and block the sender.

CHALLENGE*: Find a friend or family member who doesn't know about phishing and describe it to them. Explain to them how to spot a phishing scam and what they should, and shouldn't, do if they come across a phishing scam online.*

Photo sharing

Pretty much all social media services and websites encourage users to share photos of themselves with the world. This can be anything from a selfie to a family photo. Social media is about creating a profile of yourself for the world to see.

Some apps promise that certain uploaded videos and photos will disappear after 24 hours. Whilst this is true, it doesn't take into consideration that people can screenshot a photo and save a copy onto their own device. This could be an embarrassing or inappropriate photo of you.

There is no telling what someone can do to their copy of the photo, so be mindful that even when an app says a photo will disappear, it can live on outside of the app too.

Photoshopped

If someone refers to an image as being 'photoshopped' they are referring to the photo editing software Photoshop. A 'photoshopped' image is one that has been digitally altered and edited. This is common on fashion magazine covers where models' features are changed to create a seemingly ‘perfect’ image. There are many free photo editing apps available where users can add filters and change features to make their images look different. This can cause issues with body confidence and self-esteem especially if people are unaware that the images have been edited, as they can create unrealistic images of beauty that are not real and not attainable.

Pop-ups

Sometimes messages pop up in a small window on the screen when you open certain websites. Often the popups are adverts for products and services and other times they are phishing scams asking you to enter personal details to claim an unbelievable prize. You should avoid clicking on the popup links just in case they are unreliable or a scam. You can just close them by clicking the small x in the top right-hand corner of the popup box. It is important to look out for fake ‘close’ windows in the popup so you don’t click on something that directs you to another webpage or a risky link that can infect your device with a virus. Too many popups can be a sign that a website is unreliable.

Privacy

It is important to protect your information when you’re online and think carefully about what it is ok to share and make public for everyone to see and what it is best to keep private.

Sharing too much personal information such as your full date of birth or your full name and address could leave you vulnerable for several reasons:

- There are identity thieves who may try to steal your personal information to create an identity.
- Identity thieves may use your information to pretend to be you online.
- There are some people who want to harm and harass others online.

Don’t make your telephone number, details of the school you go to and home address public.

Make sure you check your privacy settings on your social media account regularly to ensure you know what is kept private and what is shared in public.

***CHALLENGE**: If you have social media accounts, think about the information you have shared. If you think you have shared too much on your profile, adjust your privacy settings and remove some of your personal information.*

Privacy Settings

Social media apps such as Facebook and Instagram allow you to look at, and change, your privacy settings, so you can stay safer online. The privacy settings allow you to decide how much other people can see of your information.

Privacy settings on apps vary depending on what their main use is, but the core options you should be given include:

- Deciding if everyone, just your friends or no one, can see what you’ve posted.
- Choosing who can send you friend requests.
- Turning search features on or off. Some apps allow people to find each other using email addresses or phone numbers.
- Choosing location settings. Some apps allow people to find out where their friends are. This can be risky as strangers may also be able to see where you are or where you go to school. It is advisable to switch your location settings off.

What you need to remember is that even after you’ve set up your privacy settings for all your different social media accounts, they need to be updated regularly. Some sites such as Facebook and Twitter are constantly changing their privacy settings as they grow bigger and more people use their services.

You will usually be informed that there have been some changes and it will remind you to revise your privacy settings. But, remember, just because you’ve set them once it doesn’t mean that they’re set for life.

CHALLENGE: *Sit down with a trusted adult and look through all your privacy settings on any apps or accounts you use. How can you adjust the settings to make your information more private and secure?*

QR code

QR code is a trademark for a type of barcode first designed in Japan. This is a type of barcode, which is a machine-readable label. The label is scanned and contains information which is attached to it. For example, many travel tickets are now readable through a QR code that can be scanned straight from a smartphone or other device and contain all the travel booking information. Many websites and advertising campaigns use them to direct people to further information.

Recovery

It is important to learn how to recover from any mistakes or things that go wrong online so that you can go back to enjoying the digital world and making the most of all the opportunities the online world has to offer. Recovery is a key part of digital resilience. Here are a few key points to remember:

- Always tell a trusted adult if you come across anything that upsets or scares you online.
- Report any bullying or abuse to a trusted adult so that they can help you fix it.
- If you post something and realise it probably wasn’t a good idea, delete it straight away.

- If you post an image of a friend and it upsets them, make sure you take it down and apologise.
- If you've shared your password with someone else, then change it to a stronger and more secure one.
- Check your privacy and location settings on all your accounts to make sure they are private, and you know who you're sharing your information with.

***CHALLENGE**: Think about a time you may have made a mistake online and make a note about how you could avoid it happening again.*

Reporting

It is important to work out how to report abuse on any online services that you use. Most reliable websites should have a clear indication of where you can go to report anyone or anything that you see that is harmful or upsetting. Social media companies employ moderators who aim to ensure any reported abuse or harmful posts are dealt with.

***CHALLENGE**: Sit down with a trusted adult and work out how you could report abuse on the apps and websites that you use. Make a note of these in simple steps so that you know what to do if something were to go wrong online. Decide what your 'recovery' strategy would be in different online scenarios where things have gone wrong. What steps would you need to take to recover?*

Risky

A risky behaviour is one that is potentially dangerous and could cause someone harm. In this curriculum the term risky contact is used to refer to messages from strangers online. Not all contact from strangers is dangerous, but it is risky because of the possibility that it may lead to harm. It is important to avoid sharing personal information with strangers online.

Scam

Some people online may try to trick or cheat others into doing something. This may be tricking them into giving away personal information or even trying to get money from them. The curriculum includes information on how to spot phishing scams. It is important to learn how to watch out for scams online and look for clues that show something may be a scam.

Screenshot

This is also known as a screen capture. If you take a screenshot, then you capture an image of what is displayed on the screen at the time. You can do this on most devices including smartphones. This can be useful if you need to keep evidence of any trolling or bullying messages.

The ability to take screenshots can also be considered a risk because people are able to take a copy of an image that you may have posted assuming that it would disappear after a certain amount of time. This is a feature promised on some apps where images are said to disappear after 24 hours.

Search engines

The internet has search engines to help you find information. You can type in key words online and expect to be provided with a list of website options to visit. There are lots of search engines that you may have heard of including Yahoo and Bing. The most popular search engine in the world is currently Google. Google deals with trillions of searches each year from all over the world.

Selfie

This is simply a photo you take of yourself, usually one taken with a smartphone or webcam and often shared via social media.

Snapchat

This is an image messaging and multimedia app where you can send photos and create digital stories.

On Snapchat you can:

- Send snaps (photos or videos lasting up-to 10 seconds).
- Create your own snapchat story (which lasts up to 24 hours).
- Find friends within your mobile phone contacts.
- Use filters to make your photos and videos fun and exciting.
- Talk to your friends using the messaging section of the app.
- Find out where your Snapchat friends are using Snap Map, but these location settings can be turned off to help keep you safer when using the app.

Social media

This includes websites and applications that allow you to create and share content or to participate in social networking. Some popular sites include Facebook, Twitter, Instagram and Snapchat.

Streaming

Streaming means listening to music or watching video online in real time, instead of downloading a file to your computer or other device and being able to watch it later.

Streaming requires a fast internet connection to show the data in real time. With internet videos and webcasts of live events, there is no file to download, just a continuous stream of data.

Some streaming of content online is legal, but it is possible to illegally stream films and music from illegal websites that may have access to copies of films that are still being shown in the cinema or live streams of sports games. The quality of the stream may be poor and the websites streaming illegal content are usually unreliable with pop-up adverts and links that may contain viruses that may infect your device.

Trolling

Unfortunately, just like in the offline world, some people can be unkind online. Sending nasty messages online is not difficult and can be done anonymously. People who send these messages are often known as internet trolls. The act of writing abusive and inflammatory messages with the aim of provoking and upsetting others online is known as trolling.

Internet trolling is the act of deliberately writing offensive, nasty, messages and comments with the aim of making other people angry, upset and/or react to the comments.

An internet troll will often target a public figure they have never met and write comments, so they can get into an online debate or argument with others. They sometimes act anonymously or use a fake identity.

If you come across a troll online, it is best not to engage with them, as this is just what they want. If they are saying something offensive and upsetting, you should block and report them. You should also tell a trusted adult, so they can support you.

If you receive a nasty message online, it is ok to feel upset and angry. You may feel the need to reply to them with a rude response. But, this will only make things worse. People send unkind messages in order to get a reaction. If you respond to them and get into an argument, then you will be doing exactly what they want you to do.

What should you do instead?

- Tell a trusted adult what has happened, so they can support you.
- Block and report the person using the security tools available on the website or app.
- Don’t delete the messages until you have copies of them to show as evidence.

***CHALLENGE**: Come up with a simple definition of the word trolling and explain it to at least one other person, perhaps a parent or a sibling. Have you ever seen evidence of online trolling? How did you react?*

Twitter

This is a website where users send out short messages known as tweets to let the world know what they're doing in real-time.

On Twitter you can:

- Publish tweets in 280 characters or less.
- Follow other tweeters.
- Get followed back.
- Upload photos, videos and GIFs (animated images).
- Retweet other tweets, meaning you share their tweet for your followers to see too.
- Live stream using Periscope.

Two-step verification

Two-step verification is an optional security feature that you can enable for many online accounts for example WhatsApp or Facebook. It can usually be found and enabled under the settings tool.

When you enable two-step verification you add an extra layer of security to your account because you need to do two things to access your account. It is like having to open two doors with two different keys before you can enter a room.

It is particularly useful if someone manages to get hold of your password without you realising as they will be unable to get past both steps and access your online account with just your password.

Here is a common example that some online accounts offer:

- Step 1 – enter your password to the account (something you already know).
- Step 2 – enter a secret code or pin number (something that is generated and sent to your phone).

***CHALLENGE**: Research two-step verification and activate it for at least one account to make it harder for anyone else to access.*

Unreliable

Something unreliable is untrustworthy and may not be true. This curriculum refers to 'fake news' as unreliable information. It is important to learn how to spot the signs that something you see online is unreliable. It is not always easy to spot fake news but most of the time there are some clear clues.

URL

A URL is an acronym that stands for Uniform Resource Locator. The URL refers to a web address on the internet. If someone asks you to type in the URL or check the URL to make sure it is secure, they are referring to the web address. E.g. www.telenor.com. It can also be referred to as a web link. If the URL looks strange, with lots of numbers and jumbled up characters, it may not be a legitimate or reliable site.

Virtual currency

This is also known as virtual money and is a type of unregulated, digital money, which is issued and usually controlled by its developers. It is used and accepted among the members of a specific virtual community.

Vlog

A vlog is a video blog. There are some very popular and famous *vloggers* who have many followers. Popular vloggers are lifestyle, music and beauty vloggers along with people offering peer-to-peer support.

WhatsApp

WhatsApp is a mobile messaging app which allows people to exchange messages to their phone contacts, whilst online, without having to pay text message fees. On WhatsApp you can:

- Create groups and send messages, images, videos and other files.
- Have instant message conversations with contacts.
- Make face-to-face video calls.
- Send voice recordings.
- Voice chat across the internet – like a phone call.
- Send instant messages online from a desktop computer using *WhatsApp web*

Website

A website is a collection of related web pages usually under a common domain name. Public websites are accessed via the internet whereas private ones, such as websites specifically for employees of one company can be accessed internally via the *intranet.*

There are many different types of website. For example:

- Company websites e.g. www.telenor.com
- Blogs: fashion, travel, news, entertainment websites
- Social networking websites e.g. facebook.com

WECHAT

WECHAT is a messaging app, a bit like WhatsApp, which allows people to exchange messages. It also has some extra features. On WECHAT you can:

- Create groups and send messages, images, videos and other files.
- Have instant message conversations with contacts.
- Make face to face video calls.
- Send voice recordings.
- Voice chat across the internet – like a phone call.
- Send instant messages online on a desktop computer.
- Play games.
- Search for other friends using geo-location feature.
- Post images and messages on a mini blog called ‘moments’ for contacts to see.