Tech it Out

Staying safe on the internet

Thera East Anglia®

Cambridgeshire County Council

Innovate & Cultivate Fund

We have received support from the Cambridgeshire Community Foundation

Tech it Out

What is Tech it Out?

project

online

confidence

Tech it Out is a digital inclusion project funded by the Cambridgeshire Innovate and Cultivate fund which aims to support adults with a learning disability who live across Cambridgeshire to get online.

The aim is to build confidence and reduce anxiety while exploring a wider online community. Thera East Anglia is working together with Cambridge Online and The Good Things Foundation to carry out the project.

How to use this leaflet

guide

safety

This guide is about how to stay safe online whilst using the internet and social media.

It will help you to understand some of the risks of using the internet and how to share any safety concerns that you might have.

Version 1.0, Feburary 2022

Tech it Out

Contents

What do people do online?


fun

People use the internet for lots of fun things. You might use your social media or internet to do things such as:


talk

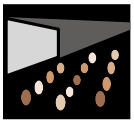
Talk to your friends


sports

Watch sports


music

Listen to music


movies

Watch films

online shopping

Do online shopping


family

Keep in touch with family

What is online abuse?

abuse

Though the internet can be a lot of fun and very useful, people can also suffer from online abuse when using the internet.

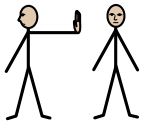
internet

Online abuse is any type of abuse that happens on the internet.


distress

Abuse happens when someone acts in a way that causes harm and distress to others.

Types of online abuse


discrimination

Discrimination

This is when someone is abusive to you because of your race, gender, age, sexuality, religion, appearance, or disability.


exploitation

Exploitation

This is when someone abuses you to get something out of it for themselves. Matecrime, sexting, and financial abuse are types of exploitation.


Psychological

Psychological

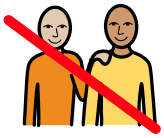
This is when someone tries to effect your emotions by abusing you. Verbal abuse, trolling, cyberbullying, and controlling behaviour are types of psychological abuse.

What does online abuse look like?

MATE Crime

What is it?

MATE crime is when someone says they are your friend, but they do things that take advantage of you. MATE crimes often happen in private and are not seen by others.



A ‘mate’ may be a friend, family member, supporter, paid staff or another person with a disability. You might have met them recently or you might have known them for a long time.

What does it look like?

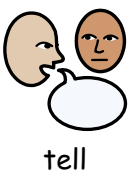
The person normally starts by saying they are your friend but they then go on to do things that are harmful to you.

For example they may:

- Borrow your mobile phone and use up all the credit
- Ask you to pay for everything when you are out with them
- Take money from you without asking
- Force you to do things that you do not want to do
- Call you names when they see you or send abusive text messages

What should I do if I feel uncomfortable?

If someone who says they are your friend hurts you, steals from you or makes you do something you don’t want to do, you should tell someone you trust right away.



Mate crimes are Disability Hate Crimes and should be reported to the Police. Tell someone that you feel comfortable talking to and they will support you to report it to the police.

Version 1.0, Feburary 2022

Cyberbullying

What is it?

what

Cyberbullying is when someone makes fun of another person online or picks on another person through emails, social media, text messages, or online forums.

messages

Cyberbullies are often called “trolls”. Trolls may send you messages online that are hurtful, embarrassing or threatening.

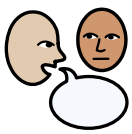
What does it look like?

bullying

Online bullying behaviour includes:

- Being teased or made fun of online
- Unpleasant comments being posted about you
- Pictures or videos of you being shared publicly online that you don’t want to be seen
- Blackmail (pressuring you to do something by threatening to post things you don’t want to be seen)
- Someone using your username and password to pretend to be you to hurt someone else
- Someone using your username and password to pretend to be you to post embarrassing things.
- Someone asking you to do things that make you feel uncomfortable, like send them a naked picture of yourself

uncomfortable



tell

What should I do if I feel uncomfortable?

If you feel like you are being bullied online, talk to someone that you trust. They will be able to support you to report the messages to the online platform or the police if necessary.

Version 1.0, Feburary 2022

Sexting

what

What is it?

Sexting is when you or another person sends, forwards or receives pictures, videos or messages of a sexual nature of any kind. These can be sent for several reasons including:

photos

videos

- Flirting with another person
- Pressure from friends
- As part of an intimate relationship
- Or even for revenge

danger

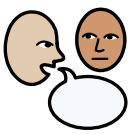
Dangers of sexting

- Even if you wanted to send the images or videos at first, you may later regret doing this which can cause negative feelings and emotional hurt
- If you share sexual photos or videos of yourself with someone, the other person may end up showing them to other people or put them online where strangers can see them
- Some people may use apps such as Snapchat for sexting because they believe that the image or video can be sent and then will disappear forever. However this is not true and files can be saved, screenshotted or even recorded.

uncomfortable

What should I do if I feel uncomfortable?

If someone asks you to send sexual images of yourself, you should ask them to stop and tell them you are not comfortable doing that.



tell

You should then tell someone you trust so they can support you through the situation which may include reporting them.

Version 1.0, Feburary 2022

Inappropriate or explicit content

What is it?


inappropriate

Online pornography - Whether you have looked for or accidentally found online pornography, you may find the content confusing or distressing.


distress

When you look at online pornography, you risk exposure to graphic, violent or misleading messages about sexual practices and gender stereotypes which could lead to the wrong idea about sex and intimate relationships.


distressing content

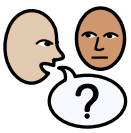
Graphic image or videos - Wherever you can view or share content, there is a risk that you may see something distressing or worrying.


anxious

Graphic content can be distressing to see and may make you feel scared, anxious or leave you with questions or fears about your own or others safety.

Many apps and sites have moderators in place to help remove inappropriate content, however some don't.

How to avoid inappropriate or explicit content



ask

If you are worried about seeing content you may find distressing on the internet, you can add a safety filter to your device or internet that will filter out inappropriate content.

Ask someone who supports you for help with doing this. Some gudiance on adding a filter through your internet provider is here. https://saferinternet.org.uk/guide-and-resource/parental-controls-offered-by-your-home-internet-provider

Online Scams

What are they?

what

Scams can come in many forms, but all are designed to get hold of your money. Scams try to get you to give somone your personal details or even try to trick you into giving someone your money.

scam

scammer

Scammers will pretend that they are protecting you, or doing you a favour by promising offers that will save you money. However, they will often try to pressure or even frighten you into doing what they want. For example, they may say you need to pay for something now to avoid missing a good deal.

What do they look like?

Phishing emails and text messages

phishing scams

Phishing scams trick you into giving someone your passwords or personal information. This is usually through an email or website that claims to be from a company you know.

form

The emails may look very real and have the right logos, colours and images. The email will usually ask you to sign onto a website, click on a link, or enter information into a form.

personal details

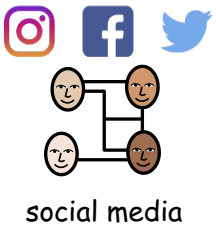
However, if you follow the instructions, you will actually be giving the scammer the information they need to access more personal information, steal your identity or take money from your bank account.

Version 1.0, Feburary 2022

How to spot a phishing email

Your email or message may be a scam if:

- It it has been emailed to lots of people and not just you. You can check this in the “recipients” box of the email
- Your name in not used the email
- The message contains spelling mistakes or bad grammar
- The link address does not look right. Hover your cursor – **without clicking** – over any links in the email or on the website. Look down in the bottom-left corner of your browser as you do so, you should see the full address of the website that the link will take you to
- Remember that your bank will never ask you for your bank details or log in details through an email or message



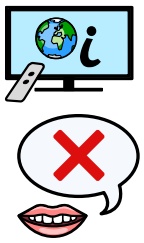
Social Media and Messaging Apps

Social media and messaging apps, such as Facebook or WhatsApp, can be used to scam you. Scammers may promise special offers or vouchers if you click on a link or fill out a survey.

How to spot a social media scam

- Check if you recognise the company name or brand - names you do not recognise are more likely to be a scam
- If a friend seems to be sharing lots of unusual messages don’t click on the link, they may have been hacked
- Reach out to the organisation or company through their official social media accounts or email to check if the offer if real
- If in doubt, ignore the post or message or report it the online platform.

Fake News



Fake News is news that is not true but lots of people see it on social media, they believe it and then share the information with others. In fake news, the facts, photos, and videos by be changed. By sharing these posts, you may spread false facts to others.

How can you spot fake news?

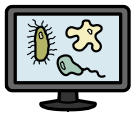
It is difficult to spot fake news but you can check where has the news article come from. It is more likely to be real if it is from an organisation that you can trust such as the BBC.

If you are not sure whether the article can be trusted, it is best not to share it with others

What can you do if you see fake news?

if you start receiving fake news, the most important thing is not to share it, like it or spread the information.

Viruses, Malware and Spyware



Viruses, Malware and Spyware are programmes that are downloaded onto your computer to destroy files and data, stop your PC working properly, or give scammers access to the personal data on your computer.

How can you spot if you have downloaded malware?

Signs to look out for include

- A computer that is running slower than it should be
- Your internet connection suddenly slows down for no reason
- Your apps and programs stop working properly

How can I protect against malware, spyware and viruses?

- Ensure that you have anti-virus software installed and running on your PC
- Use a password manager to ensure that you have strong passwords that are hard to guess

Other Scams

Other common scams include:

- Fake emails from the HMRC around March and April time
- Parcel delivery scams especially near Christmas time
- Fake Covid-19 related emails and phone calls appearing to come from the government, the NHS, the HMRC or the Track and Trace programme, but are actually phishing attempts or attempts to infect you with malware

Staying safe dos and don'ts

Do ✓

Create strong usernames and passwords

- Include a mix of upper and lower case letters, symbols and numbers.

Keep your computer and other devices secure

- Keep your device up to date. Your computer, tablet or mobile should notify you when a new update is available.
- Install an anti-virus software onto your computer to keep it safe.

Protect yourself when shopping online

Some things you can look out for include:

- A padlock symbol in the URL bar at the top
- The address should start with 'https'

Stay safe on social media sites

- Avoid sharing personal details such as your telephone number or home address
- Go into your settings and ensure your privacy options are set how you'd like
- Only add people you know

Have someone support you

- Go online with someone you trust

Log out

- Remember to log out of your apps and websites when you are done using them

Staying safe dos and don'ts

Don't ✕

Don't share your password
- Make sure to change them regularly too regularly

Don't give away your personal details
- Never give out your location, your address, or where your live when you are online

Don't accept strangers as friends

Don't use the exact same password for every account and profile you have online

Don't click on links or pop-ups if you haven't heard of the site

Don't download anything illegally

Don't make purchases whilst connected to public Wi-Fi
- Use your phone's network or wait until you are back at home

Version 1.0, Feburary 2022