A Guide To
Staying Safe Online

Solihull Safeguarding Adults Board
Protecting Adults Together

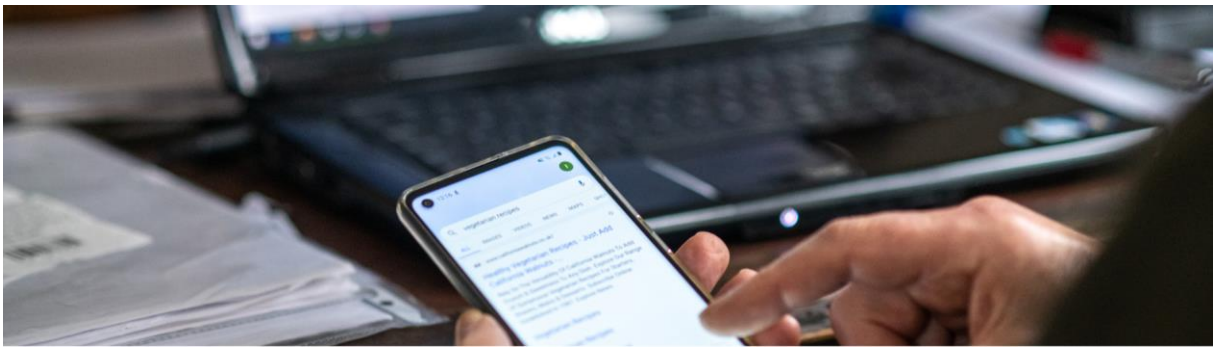
Contents

Click on each heading to go to the relevant section

Introduction

The internet is a brilliant place to connect with others, to be creative, and to discover new things. However, the internet is always changing, and being able to keep up to date with technology can be challenging.

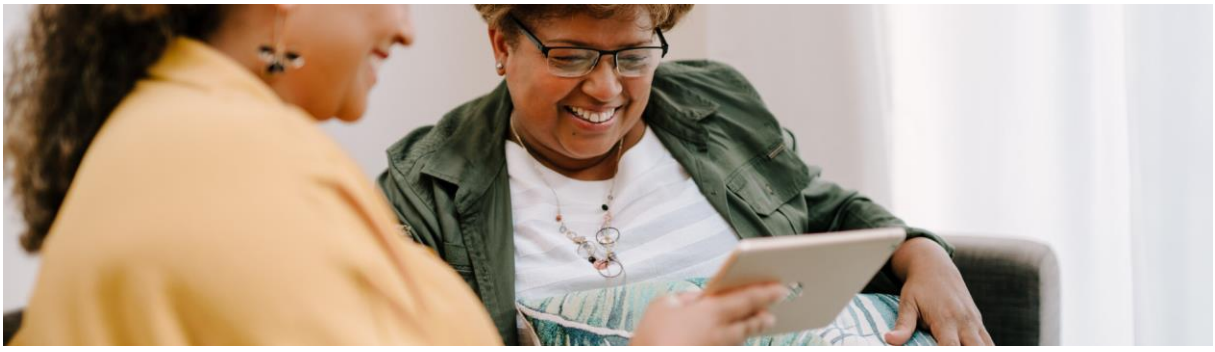
The resources and tips in this guide are intended to help everyone use the internet safely, responsibly, and positively.



Remember

If you are worried about someone's immediate safety you should call 999.

Safeguarding concerns about adults with care and support needs who are experiencing, or at risk of, abuse should be referred to Solihull Adult Social Care One Front Door – by calling 0121 704 8007 or via the online referral form



What Are the Issues?

Conduct: The Information People Share Online

People need to be aware of the impact that their online activity can have on both themselves and other people, and the digital footprint that they create on the internet. It's easy to feel anonymous online and it's important that people are aware of who can view, and potentially share, the information they may have posted. When using the internet, it's important to keep personal information safe and not share it with strangers.

TOP TIP

Discuss with individuals you are working with, the important of reporting inappropriate conversations, messages, images, and behaviours and how this can be done.

Content: Access to Age-Inappropriate or Unreliable Content

Some online content may be hurtful or harmful. This is true for content accessed and viewed via social networks, online games, blogs, and websites. It's important for everyone to consider the reliability of online material and be aware that it might not be true or written with a bias.

TOP TIP

Individuals may need your help as they begin to assess content in this way.

Contact: People Can Be Contacted by People Who Seek to Groom or Abuse Them

It is important to understand that new friends made online may not be who they say they are and that once a friend is added to an online account, they may be able to see personal information. Regularly reviewing friends lists and removing unwanted contacts is a useful step. Privacy settings online may also allow individuals to customise the information that each friend is able to access.

TOP TIP

Reinforce with the people you are working with, the importance of telling a trusted adult straight away if someone is bullying them or making them feel uncomfortable, or if one of their friends is being bullied online.

Commercialism: People Can Be Unaware of Hidden Costs and Advertising in Apps, Games, and Websites

People's privacy and enjoyment online can sometimes be affected by advertising and marketing schemes, which can also mean inadvertently spending money online, for example within applications.

TOP TIP

Encourage individuals to keep their personal information private, to learn how to block both pop ups and spam emails, and to turn off in-app purchasing on devices where possible.

Online Grooming

Online grooming is where someone befriends a person online and builds up their trust with the intention of exploiting them and causing them harm.

Harm caused by grooming can be sexual abuse, both in person and online, and exploitation to obtain sexually explicit images and videos of the person.

Grooming techniques could also be used as part of the radicalisation process or to obtain financial information from the person.

How Does 'Online Grooming' Happen?

Grooming can take place over a short or long period of time. It can start out publicly on social media and in games but will most likely move across to private chats.

Anyone could unfortunately groom a person online, regardless of age, gender, or race. Groomers are very skilled at what they do and can often befriend a person by appearing to have the same hobbies and interests as them. Using fake accounts and photos, they may also appear to be the same age as the person. However, not all groomers will choose to mask their age or gender. Some groomers may impersonate an aspirational figure such as a modelling scout, sports coach, celebrity, or influencer, whilst others may use their age and experience to develop a 'mentor' type relationship with their victim.

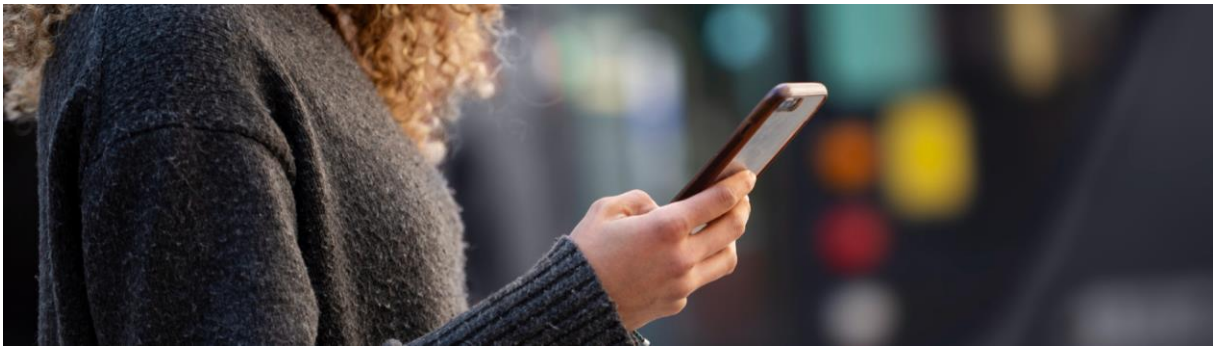
A groomer will use the same sites, games, and apps as the person they are grooming in order to gain their trust and build a friendship. People can be flattered at first by the attention given to them by this new 'online friend', particularly if they are offering support, showing

understanding, or giving validation. However, they may also seek to manipulate, blackmail, and control the person, potentially isolating them from their friends and family.

It's important to remember that people may not understand they have been groomed or see their 'online friend' as untrustworthy or abusive.

'So you got naked online' is a guide to help young people and those supporting them deal with issues resulting from sexting

Stop It Now produced an easy to read guide to Adult Grooming - I have made a new friend online. This guide points out the warning signs that might indicate that someone isn't who they say they are online.



Intimate Image Abuse (a.k.a. Revenge Porn)

Intimate image abuse is the act of sharing intimate images or videos of someone, either on or offline, without their consent with the intention of causing distress.

Intimate image abuse can also be referred to as 'revenge porn', non-consensual pornography or image-based sexual abuse.

The Revenge Porn Helpline is a UK service supporting adults (aged 18+) who are experiencing intimate image abuse, also known as, revenge porn. The Helpline was established in 2015 alongside the legislation which made it an offence to share intimate images or videos of someone, either on or offline, without their consent with the intention of causing distress.

Online Scams

Online scams are becoming increasingly sophisticated, and many people are caught out, even those who are regular internet users. Every year in the UK, millions of people lose money to scammers or unknowingly share their personal information.

Some of the most common online scams are explained below:

Email Scams

Scammers send bogus emails in the hope that people will enter their personal or financial details. They may direct someone to a fake website or trick them into thinking they've won a lottery or prize.

Some emails, known as spam or junk, may also have a link or file attached to click on or open. Opening these links or downloading the files may harm the person's device.

Scam emails can look genuine and appear to be from official places, like HMRC or a bank. There are some signs to look out for which may suggest it is a scam:

- errors in the spelling or grammar, or an unusual style of writing.
- requests for personal information, such as username, full password, or bank details - genuine organisations will never ask this.
- threats that unless a person acts now, a deal will expire, or their account closed.

TOP TIP

If you see a suspicious email, don't reply with your details, or open any links or documents. Delete the email straight away. If the email claims to be from an organisation, phone them directly using the phone number found on their official website and ask them.

If a person is worried they've been scammed they can report it to the police and to Action Fraud

Fake Websites

Scammers create fake websites which look official, requesting a person provides personal or financial information. For example, a fake bank website may be set up asking a person to update their account or security information. Often, they will look very similar and only a few details may be different.

There are also websites set up to look like a copy of a service offered by government websites. For example, websites which offer to help people apply for a passport renewal or a new driving licence. Although they are not illegal, these websites charge extra money if used, rather than going directly through the official government department where the service is free of charge.

TOP TIP

Visit your bank's website by typing their official web address in your internet browser – you can find this on letters from the bank.

If you aren't sure about which website to use for a government service, go through GOV.UK, the Government's official website, to find what you need.

Age UK Staying Safe Online - Advice on how to protect yourself by knowing what to look out for, and what to do if you suspect a scam.

Computer Viruses

Computer viruses (sometimes called malware) are rogue programs that spread from one computer to another. People may be sent an email with an attachment, which when they click on it will release a virus.

Criminals can then use this to take control of a computer, or the virus may scan the computer for personal information. It can also slow a computer down, send out spam email or delete files.

A person may even get a phone call from someone claiming to be from a well-known software company, like Microsoft, saying there's a problem with the computer and needing to get access to it, including personal details. Legitimate IT companies never contact customers in this way. This is a common phone scam – hang up straight away.

TOP TIP

Use anti-virus and anti-spyware to protect your computer from viruses.

Relationship Scams

Scammers can use social networks like Facebook or dating websites. Once they've gained a person's trust they'll start asking for money, often by telling an emotional or hard luck story.

These tricks are hard to spot, so it's always worth talking to a friend or relative about it, especially if things seem to be moving fast. Be careful if the person starts moving away from the chat room or dating site to communicating by email or text message.

TOP TIP

Never send the person money or give them your account details. If you arrange to meet, make sure it's in a public place, tell someone else where you're going and don't give away information too quickly.

Health Scams

False and misleading claims may be made about medical-related products, such as miracle health cures, and fake online pharmacies may offer medicines cheaply.

However, the actual medicine delivered can turn out to be poor quality and even harmful to health.

TOP TIP

Check if an online pharmacy website is legitimate by clicking on the 'Registered Pharmacy' logo on the website's home page – this should lead to the General Pharmaceutical Council website.

Money Mules

Criminals may approach an individual online and ask them to receive money into their bank account and transfer it into another account, keeping some of the cash for themselves. This is known as being a money mule and constitutes money laundering, which is a crime. Mules will usually be unaware of where the money comes from – fraud, scams, and other serious crime – or where it goes.

TOP TIP

Be cautious of unsolicited offers of easy money. If it sounds too good to be true, it probably is. Be wary of job ads that are written in poor English with grammatical errors and spelling mistakes.

Don't be fooled is a partnership between UK Finance and Cifas. It aims to inform students and young people about the risks of giving out their bank details and deter them from becoming money mules.

Social Media

Social media is a website or app that enables users to communicate and engage with others online. Users can share information such as posts, pictures, or videos, and others can respond through varying levels of engagement such as comments, reactions, or 'likes'. From keeping in touch with friends and family to watching videos, reading blogs, listening to podcasts, and creating web content, the options available through social media are endless.

However social media can also be used by those wishing to cause harm to others, through cyber bullying (bullying using digital technology), grooming, identity theft or sharing offensive images and messages.

It is important individuals understand the risks of using social media and what to do to reduce these risks, whilst also feeling able to connect with friends and family online, express themselves and nurture their creativity. The following resources will be helpful in exploring using social media safely:

Enabling people with Learning Disabilities to use technology – a number of toolkits and frameworks tailored to both adults with learning disabilities and their supporters, to enable adults with learning disabilities to use technology. Developed by Open University.

Social Media Guides - UK Safer Internet Centre Find out more about the safety features available on popular social networks including Facebook, Instagram, Twitter and TikTok.

Social Media Checklists These checklists provide tips and guidance on how to use safety and privacy features on a range of social media platforms including Facebook, Twitter, Instagram, and Snapchat. They have been produced by UK Safer Internet Centre Professionals Online Safety Helpline, run by UK Safer Internet Centre partner SWGfL, in collaboration with each of these social media providers and are updated regularly to reflect latest changes to safety features.

Facebook and How to be Safe this video put together by Solihull Action Through Advocacy is aimed at people who have a mild learning disability. It outlines a basic structure for personal safety awareness when joining and using Facebook.

National Cyber Security Centre Guidance on Social Media: how to use it safely. Using privacy settings across social media platforms to manage your digital footprint.

If you are concerned about content/sharing/images that are not appropriate, each social network will have their own safety tools such as reporting and blocking.

Advice about social media safety features developed by UK Safer Internet sets out key information such as reporting and safety advice for popular social media platforms and apps

West Midlands Police - Cyber Abuse - Your Options – use this link and select any of the statements that reflect the situation to get tailored advice, or view the general advice

What Can Professionals Do to Help?

Have a Conversation

It is really important to talk on an ongoing basis about staying safe online. Scammers and groomers are constantly finding new ways to trick people and online scams are changing all the time. It's not unusual for people to get tricked, so encourage them not to suffer in silence and not to be embarrassed to report it.

Not sure where to begin? These conversation starter suggestions can help:

- Ask them to tell you about the sites they like to visit and what they enjoy doing online.
- Ask them about how they stay safe online. What tips do they have, and where did they learn them? What is OK and not OK to share?
- Ask them if they know where to go for help, where to find the safety advice, privacy settings and how to report or block on the services they use.
- Ask them if they have seen people they know posting images to be mean or embarrass someone, what would they do if they saw this? Who could they go to for help?

These visual cards developed by KeyRing North Yorkshire Self-Advocacy Service are a great easy-to-read resource to support conversations around internet safety.

Skills for Care have put together this series of webinars – covering the following topics:

1. Introduction – Identifying the barriers and risks of not having access to everyday technology
2. Safety – helping people understand and balance risks and benefits
3. Technology and accessibility
4. Hardware, software, and practical technology
5. Creating good video 'spaces'
6. Supporting mental and physical health
7. Toolkit supporting people with learning disabilities to use everyday technology

Technology Enabled Domestic Violence and Abuse

Many of us rely on technology and social media to keep us connected to work, friends and the businesses or services we need. This connection is important for all of us. However, for women experiencing domestic abuse and coercive control, connecting online comes with numerous risks. Many relationships that begin romantically can quickly become controlling, with partners reading emails, checking texts and locations of social media posts. Research conducted by Refuge in 2021 found that 1 in 3 women in the UK have experienced online abuse (perpetrated on social media or other online platform) at some point in their lives.

What is Technology Enabled Domestic Violence and Abuse?

Technology enabled abuse is the use of technology to control, threaten, monitor, or harass someone. It is often experienced as part of a pattern of controlling behaviour by the abuser: many survivors experience tech abuse in addition to physical violence, sexual, economic, and emotional abuse. Abusive behaviours can include:

- Denying access to devices and technology to isolate the victim so she is unable to contact friends, family or specialist services for help and support, or to protect herself from abuse.
- Posting abusive comments about the victim on social media accounts or sending excessive amounts of voice calls, emails and texts.
- Using technology to control or manipulate home appliances, locks and connected devices.
- Using tracking devices in toys, cars, and devices to monitor locations and activities.
- Creating a fake account to harass or abuse the victim, her friends and family.
- Sending menacing messages and images that threaten the victim, her friends, family & pets.
- Sending menacing messages and images that aim to cause the victim reputational harm.
- Sharing or threatening to share intimate images without consent.

- ‘Doxing’ by posting the victim’s personal information on social media or elsewhere online.
- Accessing someone's personal accounts without their knowledge or consent with the use of known passwords or shared devices.
- Hacking children’s devices to gain full access to their accounts, or trace information such as the child’s location

This short video developed by The Coalition Against Stalkerware explains what stalkerware is, how it is installed, the signs a person may have had stalkerware installed on their devices and steps to take if a person thinks stalkerware has been installed on their device.

Resources and Help

Birmingham and Solihull Women’s Aid provides frontline domestic violence and abuse support services to women and children in the Birmingham and Solihull area.

- Call 0808 800 0028
- www.bswaid.org

Revenge Porn Helpline is a UK service supporting adults (aged 18+) who are experiencing intimate image abuse, also known as, revenge porn.

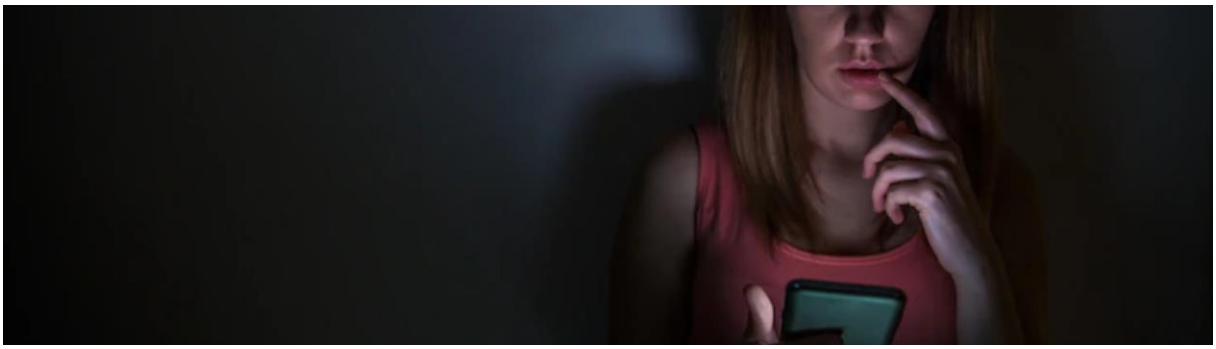
- Call 0345 6000 459
- www.revengepornhelpline.org.uk

UK Safer Internet Centre helps children and young people stay safe online

- Call 0344 381 4772
- www.saferinternet.org.uk

Safe Ireland have developed a booklet for professionals to help recognise the warning signs of technology enabled abuse, to know how to respond and to help increase the online safety of women and children.

- www.safeireland.ie/lets-talk-tech-online-safety-tips/



Safeguarding Adults Board Business Team
Solihull Metropolitan Borough Council
Council House
Manor Square
Solihull
B91 3QB

0121 788 4392

ssab@solihull.gov.uk

www.safeguardingsolihull.org.uk

Solihull Safeguarding Adults Board
Protecting Adults Together