AEM
Autism East Midlands

Advice on online safety

Online interaction can provide the opportunity to be social in a way that is easier for autistic people.

It is important that as unique individuals we have the opportunity to socialise in the ways that we feel the most comfortable.

Online safety is always something that we must consider. Here is some advice which you can use to help keep yourself safe when socialising online:

Email:

- Email is a part of everyday life and essential for both work and personal life. This means that it can be a risk for fraudulent content.
- Cyber criminals can use emails in a variety of ways; from simple spamming of unsolicited messages and attaching spyware as a file to sending unsafe links to their own website.
- Phishing is a common form of fraud committed through emails.
- This is when a person attempts to appear as a corporation or business.
- This can be very convincing, and individuals will even go so far as to using the corporation's official logo and contact information in order to trick people.
- It is important to note that official businesses will **never** ask for private information over email.

Websites:

- Websites are important tools for research, keeping up with the news and entertainment.
- Some webpages can malicious cookies or files to your device.
- They can create popup spam, redirect you to other more dangerous sites and impersonate other official companies/businesses.
- Check the webpages you are visiting are safe and reliable and be aware of the dangers of browsing the internet.
- Use Google's Safe Browsing Site Checker to see if a particular URL holds any risks
- Do not visit any unfamiliar or suspiciously named websites – For example www.a892.com
- Do not submit any personal or private information to an unknown website

- Webpages that start with https:// in their URL are secure while others with http:// are unsecure
- Regularly delete your cookies and cached files
- Do not click on any popup browsers as they are traditionally spam

Social Media:

- A great tool to communicate, share videos/images and personal updates with family and friends and make new connections.
- Be careful how much personal information you share as people may be able to impersonate your identity.
- Reduce the amount of personal data you make available on your social media profiles (Do not share your address or phone number)
- Do not add unknown people to your social media network
- Do not respond to messages or posts from persons or businesses you do not know
- Do not upload or post any sensitive content that could be used against you
- Take the time to set the privacy settings for your profile on each Social Media platform.