HONESTY EXCELLENCE AMBITION RESPECT

STAYING SAFE ONLINE

INFORMATION & GUIDANCE

(updated in response to COVID-19)

access

Your **Community** Your **Trust**

v20

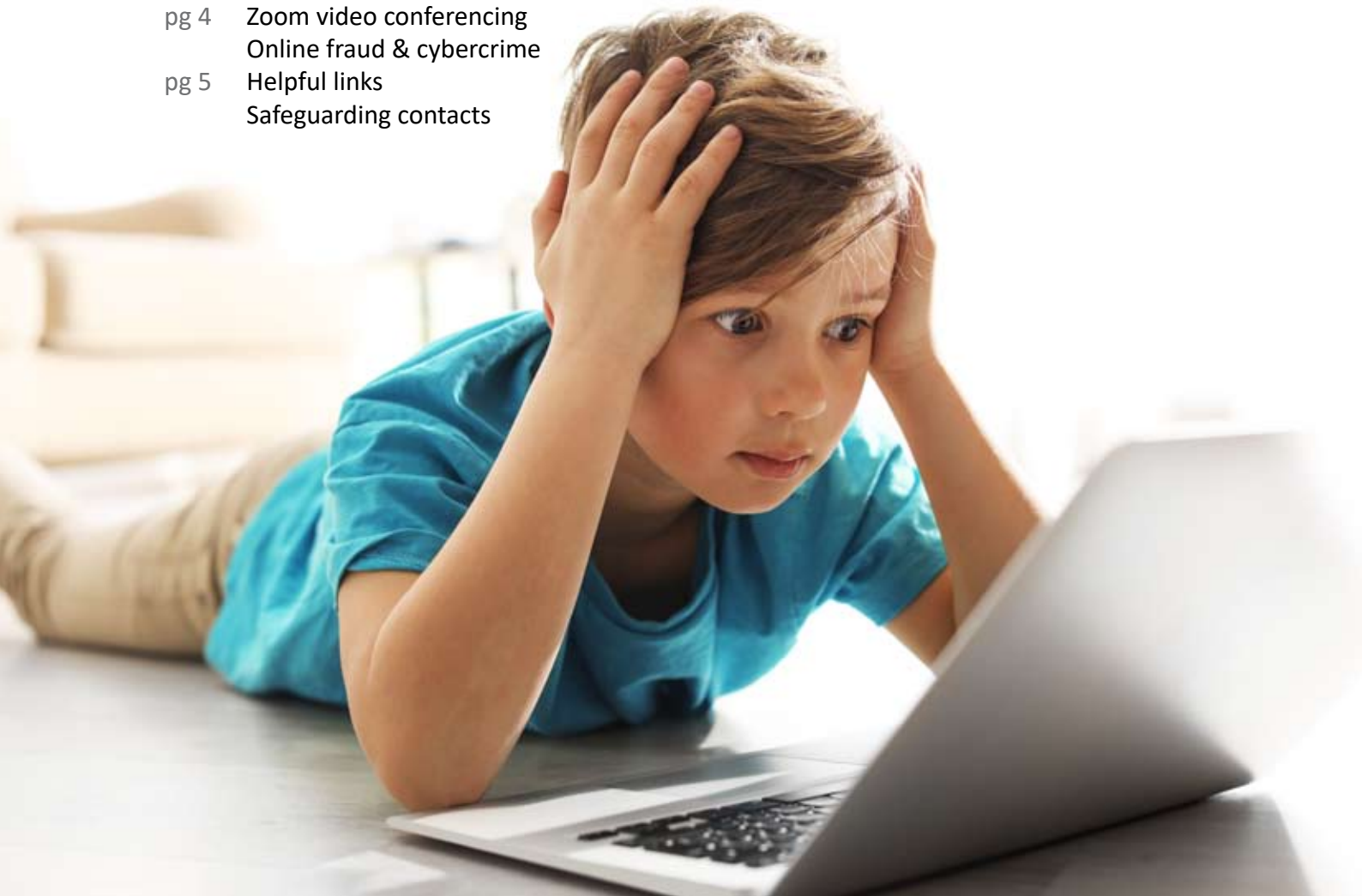
Staying safe online

The Internet is a powerful and useful tool that provides access to a wealth of information and communication. Many people are using new services, apps or devices, such as webcams and tablets, to learn/work or socialise with at this time. It is particularly important to safeguard those that may be more vulnerable to abuse and neglect, as others may seek to exploit disadvantages due to age, disability, illness or mental wellbeing.

Filtering through the mountain of safety advice and guidance available online can be overwhelming and confusing to even the most proficient internet user. To help, Access Community Trust has produced this brief document with the help of our Safeguarding Team, with an aim of providing helpful basic guidance and tips for staying safe online. We also share trusted links, where further information can be found.

As an organisation, we ourselves are using video conferencing apps such as Zoom to stay safely connected to our customers. Tips on using this platform and the measures we have taken to keep you safe while communicating with our team are also outlined.

Contents:



Keeping children safe

Most children have a positive experience of the internet, whether it is accessing educational resources, entertainment or connecting with friends and family. Spending time online can be very beneficial for children, particularly at the moment, but we recognise that many parents may worry about online safety.

Our policies are formed from advice from a number of agencies, partners and the NSPCC (National Society for the Prevention of Cruelty to Children).

It can be hard to know how to talk to your child about online safety. From setting up parental controls to advice on sexting, online games and video apps, the NSPCC website can help you to understand the risks and keep your child safe.

Visit **www.nspcc.org.uk/keeping-children-safe/online-safety/** for more information.

In addition to the above, further interactive resources, which are broken down by age group can be found at **www.thinkuknow.co.uk**. This website also has a parent/carer and children's workforce section.

Sharing information

You should be careful with how much personal information you reveal online. Sharing your address, phone number, birthday and other personal information can mean you are at a greater risk of identity theft, stalking or harassment. This includes information you post on social media.

Be wary of anyone who asks for your bank or credit card details, and only use secure sites when shopping online. Secure sites usually carry the green padlock symbol in the address bar. However, this on its own is not a guarantee that you are visiting the website you think you are. Make sure the address for the website is the one you would expect to see.

For further helpful guidance visit:
www.ofcom.org.uk/about-ofcom/latest/features-and-news/sharing-your-data-online

Privacy settings

Ensure that you adjust privacy and safety settings on websites and social media platforms to increase security and control of the personal data you share. Look for the 'privacy and security' or 'settings' on the app or website.

Factsheets to change these settings on some of the most popular platforms can be found using the below link to the UK's Information Commissioner's Office:

www.ico.org.uk/your-data-matters/be-data-aware/social-media-privacy-settings/

Passwords

Passwords are the most common way to prove your identity when using websites, apps, email accounts and your computer itself (via User Accounts). The use of strong passwords is essential to protect your security and identity. The best security in the world is useless if a malicious person has a legitimate user name and password.

Many websites and apps also offer 'Two-Factor Authentication'. This option provides an additional layer of security to your account, where an additional verification code is required. This could be sent as a text message or email to the user. If this option is available it would be beneficial to activate it.

CREATING STRONG PASSWORDS

Weak passwords can be hacked in seconds. The longer and more unusual your password is, the stronger it becomes and the harder it is to hack. The best way to make your password long and difficult to hack is by using a sequence of three random words you'll remember. You can make it even stronger with special characters.

EMAIL ACCOUNT PASSWORD

Your personal email account contains lots of important information about you and is the gateway to all your other online accounts. If your email account is hacked all your other passwords can be reset, so use a strong password that is different to all of your others.

Chatrooms

Chatrooms are a fun place to engage in discussion about a variety of topics. Whilst most people who visit online chatrooms are genuine, there are some who are there to prey on or bully other people. Take steps to keep your personal information private, be cautious when it comes to interacting with people you meet online and end communication with people who may threaten you.

Additional guidance on protecting yourself whilst using chatrooms or social media can be found here:

www.thinkuknow.co.uk/11_13/need-advice/online-friends/

Social media

There are lots of social networking websites and mobile apps that people use to chat, comment, share pictures or play games on. Sites such a Snapchat, Facebook, Instagram or Twitter, require a user to be at least 13 years old to sign up.

The NSPCC provides a comprehensive list of most platforms at a glance, together with what Experts views are of the risks with each site. View this information at **www.net-aware.org.uk**

Zoom video conferencing

Many of Access Community Trust's online services are hosted in partnership with Zoom. Whilst there are many video conferencing applications available online, we have chosen Zoom as a preference due to security and functionality.

When you join any of our conference facilities, whether it is a virtual wellbeing meetup or perhaps a 1:1 keyworker meeting, you can rest assured that these sessions are held with an Access Community Trust 'Host' that has received safeguarding training.

Our Host's manage these sessions and content to ensure the identity and safety of our customers is protected at all times. Participants are invited via secure links with passwords by email or text message.

Each session begins with introductions, where users are reminded of our online policies and ground rules. If these are violated, the Host has the option to mute or remove the participant from the conference.

Guidance on downloading Zoom to your device:

Online fraud & cyber crime

Unfortunately, criminals will use every opportunity they can to scam innocent people. They are experts at impersonating people, organisations and the police. They spend hours researching you for their scams, hoping you'll let your guard down for just a moment.

They can contact you by phone, email, text, on social media, or in person. They will try to trick you in to parting with your money, personal information, or buying goods or services that do not exist.

Law enforcement, government and industry are working together to help protect you from these criminals, by identifying fraudulent websites, preventing phishing emails, blocking phone numbers and ultimately bringing those responsible to justice.

There are simple steps you can take to protect yourself. Further information from the UK Government can be found here:

www.gov.uk/government/publications/coronavirus-covid-19-fraud-and-cyber-crime/coronavirus-covid-19-advice-on-how-to-protect-yourself-and-your-business-from-fraud-and-cyber-crime

Helpful links

Our Safeguarding team have identified a number of verified websites, where further helpful information and guidance can be found on staying safe online. Some have been mentioned throughout this document already.

KEEPING CHILDREN SAFE ONLINE

NSPCC - National Society for the Prevention of Cruelty to Children
www.nspcc.org.uk/keeping-children-safe/online-safety/

NSPCC - Guide to Social networks, app and games
www.net-aware.org.uk/

National Crime Agency - Child Exploitation and Online Protection Command
www.thinkuknow.co.uk/

SAFEGUARDING ADULTS

Social Care - Institute for Excellence
www.scie.org.uk/care-providers/coronavirus-covid-19/safeguarding-adults

PERSONAL ONLINE SAFETY

Suffolk Police Force
www.suffolk.police.uk/advice/cyber-crime/personal-online-safety

National Cyber Security Centre
www.ncsc.gov.uk/cyberaware/home

UK Government - Fraud and Cyber Crime
www.gov.uk/guidance/covid-19-staying-safe-online

UK Information Commisioner's Office (Social media privacy settings)
www.ico.org.uk/your-data-matters/be-data-aware/social-media-privacy-settings/

Safeguarding contacts

Should you have any safeguarding concerns please use the below details:

SUFFOLK
customer.first@suffolk.gov.uk
Telephone: 0808 800 4005

NORFOLK
https://www.norfolk.gov.uk/children-and-families/keeping-children-safe/report-concerns
Telephone: 0344 800 8020

HONESTY EXCELLENCE AMBITION RESPECT

access

Your Community Your Trust

Telephone: 01502 527200 | Email: admin@accessct.org | www.accessct.org
Registered Head Office | 28 Gordon Road | Lowestoft | Suffolk | NR32 1NL

Registered Charity No. 1135640
Registered Company No. 7140266