Covid-19: Safeguarding and moving services online

INTRODUCTION

This guidance has been produced to help voluntary sector organisations think through the safeguarding implications of moving their services online.

As we practice self-isolation and social distancing, many voluntary organisations are having to adapt quickly to the situation by making far more use of digital platforms to deliver their services.

Whilst these platforms can provide easy ways to communicate with people, the cyber world may be new to many users, can be daunting, and is not without risks. This is a guide to starting out in this brave new world and to keeping people safe online.

Many organisations are now running activities online through platforms, such as ZOOM, Whatsapp or Microsoft Teams. Although these platforms represent a convenient temporary solution, they do present safeguarding risks. For example, poor conduct by users in the space could make people feel uncomfortable, upset or targeted, unsuitable people could gain access to personal data about others and then use it to exploit or abuse them. Stalking, harassment and bullying can all happen online and there have already been reports of an increase in online scams relating

to the coronavirus. There is also evidence that online events are more tiring and stressful for everyone, so they may be especially challenging for some people who have mental health problems, sensory issues, and certain impairments.

As with our offline activities, it's important that we take reasonable steps to safeguard beneficiaries from experiencing harm and abuse when they engage with our services online.

As this blog from Catalyst outlines, 'no online platform is 100% safe. There are always risks. But you can mitigate them:

- Through the platform choices you make.
- By guiding and training your staff in the basics of online safety and security (at least)
- By advising your users on keeping themselves safe.

By following a robust review process that keeps your eyes on the risks. This guidance covers the following areas:

- General cyber security
- Considerations for hosting events and meetings online
- Sample advice for beneficiaries to help keep them safe while accessing your services online
- Checklist for hosting activities online

GENERAL CYBERSECURITY

Here are five cyber safety rules everyone needs to follow

1. Take passwords seriously, very seriously
2. Invest time, money, and effort in enhancing your awareness (see links below)
3. Always use a VPN (virtual private network) while browsing the web.
4. Don't download anything from a website or content provider you don't trust.

5. Be careful what you post. Think first. Words and behavior online should be of the same standards that you expect face-to-face.

For more information on general cybersecurity, see Cyber Essentials.

CONSIDERATIONS FOR HOSTING EVENTS AND MEETINGS ONLINE

1. Security

- Do some research on the different platforms that are available and only download and use software from trusted sources
- Check the privacy and data sharing settings before use
- Make sure the password for your organisation's account is strong and unique
- Make sure the hosts or facilitators check their own camera views before starting the event (to avoid displaying inappropriate attire, family photographs, etc.)
- Some platforms allow you to record a meeting, so make sure only the host can record, share the screen and show slides
- **Never** make an online event or call public. Always use a password or PIN for access or send a secure link to individuals by email or use a calendar invite. Making an event public hugely increases the risk of it being hacked, or simply joined by unverified users.
- Use the lobby feature to ensure you know who people are and verify their identify before you admit them to the room
- Consider what advice you give to beneficiaries about having their cameras on - are they comfortable with other people seeing their faces and homes? Tell them in advance how to use the blurring and background options

2. User experience

- Make sure staff test the service before the meeting or call to ensure they feel confident using the software. Check the

microphone, speaker volume, camera view and that the connection is strong enough

- Send clear instructions in advance of the meeting telling people how to join the activity and use the software. Remember, not everyone is 'tech savvy' and some may need extra support with this
- Think carefully about how long the event will be. Most people will struggle to concentrate for more than an hour. If the event is longer than that, schedule breaks for people
- Establish ground rules for respectful behaviour in the space and make it clear that anyone who breaks the rules may be removed from the virtual room
- Try and have additional staff in the room to moderate any group chats and keep an eye on things
- Make sure that you know how to remove a user just in case anyone becomes abusive or posts upsetting content
- Make it easy for people to raise concerns and provide contact details for who to speak to if they are unhappy about anything that happened during the activity
- Make sure staff have the opportunity to debrief after events to discuss issues and flag up any concerns
- Report any safeguarding incidents that happen online to the appropriate authorities (police, local authority, Charity Commission) as you would with incidents that occur offline

Resources

- NCSC: Video conferencing services: security guidance for organisations
- NCSC: Video conferencing Infographic
- Catalyst: What a youth trip to Dartmoor can teach us about digital safeguarding

- Catalyst: How to risk assess your preferred third party platform for online service delivery
- Catalyst: How safe lives uses tech to tackle domestic abuse during COVID-19
- NSPCC: Parental controls
- Thinkuknow website
- Get Safe Online
- Anti-bullying alliance: free online anti-bullying tools and training

SAMPLE CYBERSECURITY GUIDANCE FOR USERS

Here is some simple guidance which you can adapt for your users as appropriate:

Dos and don'ts

To help users stay safe in cyber space, here are some general 'rules of engagement' to follow.

When creating your account, consider these options:

DO

- Give yourself a username so you can shield your identity
- Use an avatar or other visual symbol rather than your photograph
- Set all the privacy settings to their highest / strongest options
- Make use of parental controls where there is an option and where you have children who use your devices (set parental controls on their OWN devices)
- Only respond to invitations from people you already know and don't get drawn into accepting invitations from 'friends of friends' unless you do know who they are

- Join only closed groups – some will ask you to apply and to be approved
- Send invitations to people you actually know IRL (in real life)
- Delete contacts who don't 'behave' appropriately online. Many providers have a 'Report This' option
- Keep all inappropriate messages as evidence (bullying, hate speech, stalking, incitement etc.) and report this to the police
- Use direct messaging or emails if you need to share personal information
- Help family and friends to use social media safely
- Remember that text alone isn't as expressive as speech, it lacks tone and content, and can easily be misinterpreted
- Asking for help from a young relative is a good idea, but many young people are less concerned about the safeguards that other users may wish to use

DON'T

- Make your address and other personal details or contact details public (it may affect your insurance and be open to abuse) in your profile or in open forums
- Open a message / link if you are in anyway suspicious about it
- Share a calendar that may show when you are not at home (when leaving home is allowed)
- Share / retweet / forward material that could be misleading or confusing (e.g. fake facts or myths) during the covid-19 epidemic
- Share / retweet / forward material that is likely to cause offense, including nudity, or incite hatred, persecution, or terrorism
- 'Say' online anything that you wouldn't say to someone in person

CHECKLIST FOR ORGANISATIONS

1	Do your staff / volunteers have the skills to host activities online? If not, can you provide some training or buddy them up with someone more experienced?	
2	Have you checked the security and data sharing settings on your chosen platform?	
3	Have you run some tests to make sure everything works (camera, microphone) etc.?	
4	Have you made sure the activity is secure? (password or pin protected)?	
5	Have you sent clear instructions to users about how to access the activity?	
6	Do you have enough staff to run the activity? e.g., someone to talk / present, someone to moderate the chat	
7	Have you set expectations or ground rules about behaviour in the space?	
8	If the activity is longer than an hour, have you scheduled breaks and time out for people?	
9	Do you know how to remove / delete any users whose behaviour becomes problematic?	
10	Have you informed users how to raise concerns about anything that happened during the activity?	
11	Do staff have the opportunity to debrief after the activity and discuss any issues?	

DISCLAIMER

This guidance is intended for information only. It is not a substitute for legal or professional advice and WCVA accepts no liability for any loss occasioned as a result of any person acting or refraining from acting upon it.