Guidance for working online, and online safeguarding if you're working with vulnerable people

This guidance has been compiled in partnership between the Culture, Health & Wellbeing Alliance, Arts Marketing Association, 64 Million Artists, and Real Ideas. It is designed to support anyone working online. It covers two areas: a **general guide** to meeting online, and how to make the space as welcoming and safe as possible; and **online safeguarding** if you are working with vulnerable participants or groups.

Please note that this is informal guidance, not a code of conduct or a policy, and should not be used in place of any Safeguarding Policies provided by your organisation or people who may be commissioning you to undertake work.

This is a developing document intended to adapt as practice, guidelines and resources emerge.
We welcome any comments and feedback to inform its development.
This version was completed on 24 April 2020.

Index

1. Background

Covid-19 has brought about a surge of interest in delivering activities that would normally take place in physical proximity online. These activities might include work meetings with colleagues, training, live streaming, or facilitated activities. Those of us running these sessions have varying degrees of experience and confidence in relation to online work.

We recognise that while online is an important space during a time of social isolation, 7% of households have no internet access,[1] and many people – often those with existing vulnerabilities – are unable to access or are unfamiliar with digital technologies.

We also recognise that social media in particular has positive and negative effects on mental health. The 2017 report #StatusofMind (RSPH and Young Health Movement), for example, identified increased rates of anxiety, depression and poor sleep, cyber bullying, but also improved access to information and emotional support.[2]

We would encourage you to consider whether you need to meet online, how and how often you want to do this, and how online work might connect with 'real world' activity and relationships. Please read the guidance below before moving your normal working practices online and remember to consider other options.

Some general resources

Get Safe Online provide guidance across the board, from firewalls to cyberbullying. The Open Rights Group "protects the digital rights of people in the UK including privacy and free speech online". Here is some advice on working remotely from the UK Safer Internet Centre. You might also want to read this guidance on maintaining your mental health, safety and privacy online.

Online fraud and scams

The National Crime Agency (UK) is warning against an increase in digital crime. More information can be found here: https://www.nationalcrimeagency.gov.uk/news/fraud-scams-covid19

A note on vulnerability

The section below is devoted to working with vulnerable groups, but bear in mind that all of us have been rendered more vulnerable by the sudden change of circumstance we are experiencing. Even peer group meetings may be more emotionally charged and exposing than usual. Set out to treat everyone you meet online at this time – and treat yourself – as more sensitive than usual. Bear in mind, too, that our concentration can drift during online meetings, and we may need to make more of an effort to remain engaged to support other participants.

Working online has been found to make us less inhibited with personal information.[3] Consider how you might want to respond to people this. Do you have contact details so that you can follow up with anyone you are concerned about? (Please also be transparent about saving contact details if you are doing this.) If it is an open forum, and contact details are not provided, consider how you might close the meeting so that anyone who has shared personal information feels heard, acknowledged and supported.

[1] https://www.statista.com/statistics/275999/household-internet-penetration-in-great-britain/

[2] https://www.rsph.org.uk/uploads/assets/uploaded/d125b27c-0b62-41c5-a2c0155a8887cd01.pdf

[3] Suler, J. (2004) The online disinhibition effect. CyberPsychology and Behaviour, 7(1): 323-326.

We may find ourselves in each other's homes, perhaps able to see details of people's personal lives that might not normally be available to us. Bear in mind that all of the information we gather (both consciously and unconsciously) from someone's environment informs our view of that person: their identity, social economic status, values and relationships.

If someone discloses information that makes you concerned for their or another person's safety, however, this becomes a safeguarding issue. See *Safeguarding, and your duty of care*, below, for more information.

2. General guide

Choosing the right technology

Signing up to new software is a bit like moving into a new office. Please check the software in the same way that you might inspect a space for suitability. Is it safe? Does it have what you need?

We aren't able to endorse specific software or platforms, but here are some factors to bear in mind:

- **Environmental sustainability**: Whilst online meetings still seem to be more sustainable than in-person meetings, the more complex the systems and the more they rely on heavy data use (videos for example), the more energy is used. Streaming platforms in particular have a relatively high carbon footprint.[4]
- **Data use**: How much data can you and the people you are working with afford? Some people have reliable broadband, some people rely on contracts or pay-as-you-go with mobile phone providers, which limit data use.
    - Consider whether you may be depriving people of data they could need for other things.
    - Consider the difference in data-use between software that relies on streaming video, software that uses images, and software that is mainly text-based.

  (Open Wireless has a guide to safely sharing your bandwidth with others.)
- **Accessibility**: Please see Drake Music's guidance here on accessibility for a fuller exploration of accessibility online, and this good practice guide for accessible virtual meetings from the University of Minnesota
    - how complex is the technology?
    - does it require downloading new software?
    - can it work on different phones as well as computers?
    - does the interface design support access for people with disabilities?
- **Privacy:** See below.

You might feel that you have no choice about the software you are being asked to use. Bear in mind that if you have to use a software chosen by another organisation, you can often still change its settings to suit your needs. If you feel able, please also share feedback with your hosts if you are concerned about their use of a particular software – this is a new space for many people and we will need to learn from each other as we go!

Protecting data and privacy

As we start to work with software that connects us online, we can make our personal information vulnerable to companies and to other individuals. We do the same with information from other people we are encouraging to use the same software.

[4] https://www.ourdailyplanet.com/story/your-streaming-platforms-are-coming-with-a-big-carbon-footprint/

Some software is better than others in terms of passing our information from our personal computers accessible to businesses and individuals without our being aware. Before you start working online, consider the privacy and security rules relating to the software you are using, or being asked to use. Will you be sharing information publicly, or with the company who are running the software? Do you have options in the software's settings that can make your information and that of other people using the software more private?

This is not always easy information to access, so be prepared to spend a bit of time exploring your software before using it. This Data Rights Finder created by Open Rights Group, Projects by If and the Information Commissioner's Office might be useful here. As a general rule, free programmes come with more risks.

You may want to consider using a "virtual private network" (VPN) at home. A VPN may make it harder for cyber criminals to access your computer and its stored data by using an untraceable network of servers. You can read more about VPNs on Get Safe Online, here.

Online meetings: hosting and participating

Hosting online meetings

Before the meeting:

- Does the software allow you a password option? If so, use it; this may help prevent unwanted access to your online meetings.
- Develop an agenda and a clear plan for managing the meeting. Bear in mind that – as with any meeting – the chair's role is to make sure everyone has a chance to participate.
    - Consider in advance whether this is a formal or an informal meeting – this will have bearing on whether you need to set some ground rules at the beginning.
    - Will you use an interactive format where everyone may be able to contribute, or a more webinar-style meeting that restricts who can speak?
    - Consider asking people to mute their microphones when they're not speaking – this avoids interference and background noise, which can be distracting.
    - How will you manage the conversation? Some technologies allow breakout rooms, and give you options as the host to mute people so that you can control how the conversation flows.
    - In some meetings, particularly webinar-style or larger meetings, people may choose to join or leave at arbitrary points during the meeting; do you need to consider how to manage this?
    - Do you need more than one person to manage the meeting? Some organisations are using a host 'buddy' to help manage questions and/or provide technical backup.
- Make sure you understand the technology you are using
    - What data is stored from people attending meetings?
    - How do the different meeting options work? Practise your plan with a colleague or on your own before you meet others.
- Decide whether you need to record or save anything from the meeting.
    - Why are you recording? Is it for your personal notes? for sharing with others? for sharing publicly? How will people be identified if you share recordings?
    - Bear in mind that you would not normally record every meeting.
    - Consider whether as a participant you want to be recorded.
    - *Have a backup plan* for taking notes in case participants don't want to be recorded.
    - Will you be collecting any personal data (e.g. email addresses)?

- Think about the length of the meeting. Online meetings are often more tiring than offline meetings (partly because of the extra work you are having to do to process physical cues and body language). You will probably need to make the meeting shorter than an offline equivalent.
- Think about pacing the meeting, and how you can manage everyone's input so that it doesn't become chaotic, and so that everyone has a chance to contribute. A facilitator may need to be *more* robust than in an offline space to help people understand when they can speak.
- Consider how you might manage disruptive or distracting behaviours that result from people being in their home spaces – how might it affect your meeting if someone is constantly moving around on video, for example?
- Bear in mind that in some formats people might join at random times during the meeting; how will you manage this?
- Think about where you are in your home, what you are wearing for the meeting etc.: what do you feel comfortable sharing about your life through what people can see? You might want to take down photographs of other people, for example. Consider whether you might prefer not to use video.
- Do you need to share your screen at any point? If so, don't forget to check that you aren't sharing emails or personal information by accident.
- See *A Note on Vulnerability*, below.

During the meeting:

- Explain how you are going to chair or host the meeting, explain the role of anyone else you are working with to manage the meeting, and share your agenda or plan.
- Make it clear
  - whether you are recording or saving any chat pages, or keeping a record of personal data (e.g. email addresses);
  - why you are recording or saving these things;
  - what you will do with these recordings after the meeting.
- If participants prefer not to be recorded, be prepared to take notes instead; if you really have to record, offer participants the option to leave if they prefer.
- Consider explaining to participants what you will do if the technology fails; for example, that you will try to reconnect, but that if this faile repeatedly, you will contact participants to rearrange. Wifi and broadband can fail at the best of times, and are more likely to do so during high-traffic periods.
- Some people may prefer not being visible, or may not want to share images of their homes. Offer everyone the option to use audio only.
- Make sure you allow people to introduce themselves in an ordered way so that everyone in the space is acknowledged.
- It's a tricky time to be working at home for many people, especially those with caring responsibilities. Remain focused during the meeting as much as you can, but if you need to leave temporarily for any reason, explain what you are doing; absence of attention can be magnified in online spaces and can hamper open discussion.
- Make sure you finish the meeting properly so that everyone has a sense of closure.

Participating in online meetings

Before the meeting:

- Make sure you understand the technology you are about to use
    - Have you downloaded any necessary software?
    - Do you feel comfortable using the software? If you are concerned about privacy or data breaches, you should feel free to contact the host of the meeting about your concerns, or withdraw from the meeting as necessary.
    - Make sure you know how to switch your audio and video on and off during the meeting so that you can control your own participation and how much you share
    - If you don't understand what's happening technically during the meeting, ask the host
- Consider whether you would be happy to be recorded during the meeting
- Think about where you are in your home, what you are wearing etc.: what do you feel comfortable sharing about your life through what people can see? Consider whether you might prefer not to use video.

During the meeting:

- If the host doesn't make it clear whether they are recording or saving any chat pages, feel free to check this with them
- If you prefer not being visible, use audio only.
- It's a tricky time to be working at home for many people, especially those with caring responsibilities. Remain focused during the meeting as much as you can, but if you need to leave temporarily for any reason, try to explain what you are doing as soon as you can; absence of attention can be magnified in online spaces and can hamper open discussion.

Social media

We are unable to produce specific guidance for social media given the variability and complexity of the space. There are some factors you might want to consider, however:

- Bear in mind that for some people social media is familiar and easy to use, for others it is opaque. It can be a welcoming and exciting space, but it can also be a threatening space.
- Social media is often used for personal recreation; how much of that information do you want to share if you start using it for work?
- Are you using an open platform (like Facebook or Twitter) that allows many people to see what is being posted, or a relatively closed platform (like WhatsApp)? What are the implications of the platform you are using for your privacy and that of your colleagues/participants? Spend some time exploring the privacy and security settings of the platform before you consider working in these spaces.
- If you are using an 'open' space please consider the risks of trolling. Do you understand how to 'block' people and control your privacy settings?

There is plenty of guidance out there from specialist organisations. Please find some of it below:

- NSPCC guide to child safety, including social media
- Digital Unite's guide to using Facebook safely
- Get Safe Onlie's guide to protecting yourself from cyberbullying and trolling
- Chayn's multilingual do-it-yourself guide to protecting yourself, written with people who have experienced domestic abuse in mind, but applicable to anyone

3. Safeguarding, and your duty of care

There is a difference between the good practice ideas we describe above and safeguarding. Safeguarding is about protecting the safety of the people you are working with and may involve issues upon which you have a duty to act. Safeguarding will apply particularly in the case of children and vulnerable adults.

Safeguarding policies still apply

If you are an organisation, your existing safeguarding policies for children and vulnerable adults will apply in the digital space. Please carefully review these policies with digital technology in mind to understand the implications. If you are a charity your Trustees have ultimate responsibility for safeguarding in relation to anyone the organisation works with. If you are a company, your Directors have this responsibility.

If you are a freelancer who is being commissioned to work with children or vulnerable adults, please ask them to review their safeguarding policies and help you think about how they might relate to online practice. See also 'Working with vulnerable people', below.

Working with children and vulnerable adults

In this context we use 'vulnerable adult' to an adult living with a physical or psychological condition or set of experiences or circumstances that makes them more vulnerable to challenging experiences.

Just as with a face-to-face meeting, if you are going to be working with vulnerable people, you need to have a current DBS (Disclosure and Barring Service) check. Please see the government guidance here and be sure to check what level of DBS you need.

Before you start planning, can you answer 'yes' to these questions?

- Do you or your commissioner have robust safeguarding policies and procedures in place? Do you know how to use them?
- Has a risk assessment been done for working in other people's homes, or at least for delivering frontline face-to-face work? (many of the same considerations need to be considered when doing this online)
- Have you considered your own and your participants' level of IT literacy? You may need to blur backgrounds, avoid showing family photos on walls etc., and make sure you consider GDPR if you are screensharing (avoid having emails open etc).
- Does the software you're using hide other people's contact details with the other users who are on a group call at the same time? Do you risk giving away individuals personal contact details?

If the answer to any of the above is no, please find an experienced partner organisation with the right policies in place to create safe working environments for online outreach work to happen rather than trying to upskill to make this work for yourself.

Is there an easier, safer way to do it? **Not everything needs to happen online!**

Safeguarding and Disclosure

Processes to tackle safeguarding and disclosure (i.e. what happens if someone reveals information about themselves that indicates they may need further support) will be covered by your organisation's safeguarding policy or the policy of the organisation commissioning you.

You should be trained in safeguarding handling disclosure before you work with children or vulnerable people on- or offline. If you are being commissioned to undertake work and you are not familiar with safeguarding and disclosure procedures please discuss this with your commissioner before undertaking work.

Bear in mind that disclosure *may take other forms* online. It may be that you can see or hear evidence of activity that concerns you in someone's home, for example. Many safeguarding policies were created prior to the upsurge in online activity, so you may need to discuss this with your designated safeguarding officer before you start working with the group or person.

Disclosure guidance often relies on being able to refer people to local services if they need additional support. Online offers an opportunity to be open to participants from further afield but it's important to consider the risks of working with people who won't be able to connect to these local services, and how you will deal with those risks.

Research suggests that some people self-disclose or act out more frequently or intensely online than they would in person due to distancing factors. Younger people or psychologically vulnerable people may be particularly prone to what's known as online "disinhibition".[5]

Setting up and running meetings or group sessions

For general guidance on setting up and running online meetings, refer to 2 (General Guide), above.

In addition to this if you are working with children or vulnerable adults, you might want consider the following:

- How might you organise some supervision (including peer supervision) for yourself?
- Sessions may be more tiring online than in person. You are likely to be able to do less than you might expect to face-to-face (this is not a failure of facilitation!)
- Remember that many platforms are designed with data (rather than human beings) in mind and have all sorts of functionality which is superfluous or might exclude people. Ask yourself whether you really need to use functions such as chat, slide-sharing, or voting just because they're there.
- Spend a period at the start of the session (as you would offline) establishing an agreement for how you will work together. By having a loose contract with participants that everyone can add to, you will be establishing a culture of trust and safety. Consider whether it is appropriate for confidentiality to be agreed between participants, for example. Inviting people to share only what they feel comfortable with, for example, signals that it is not expected that participants share personal or emotionally sensitive information about themselves.
- It is especially important that you fully understand the software you are using
  - to choose software that meets your participants needs and does not create additional anxiety about learning new skills or expending unnecessary data
  - to protect the privacy of your group's members
  - to support your ability to facilitate with confidence

[5] Suler, J. (2004) The online disinhibition effect. CyberPsychology and Behaviour, 7(1): 323-326.

- Does your software enable participants to ‘direct message’ each other without the host being able to see the messages? If so, you may want to consider disabling this option, which could limit your ability to safeguard participants.
- During challenging or stressful times, it may be more appropriate to build in check-in time for participants to report on how they’re feeling. This is supportive at both the beginning and end of sessions. Try not to squeeze out this reflective space due to other activities running on. Reflective time at the end of a session in particular helps ground us and give a sense that we have engaged, been recognised and listened to.
- Consider too how you might or might not follow-up after the session with the participants.
- Think about what reflective practice you can build in for yourself; can you write notes after the session? Is there someone you can debrief with?

Facilitators have a duty of care to look after the needs of the whole group. We need to think what our response will be if a participant joins an online group in a state of undress, eating and drinking, on their bed, playing with pets and children, or behaving antisocially, for example. People suddenly leaving a group, or getting up and leaving the room might be irritating or even quite triggering for some participants. Likewise with distracting notifications or sounds in the environment. We may need to establish and uphold boundaries more robustly than we would in person – something that might be quite challenging for some of us. The rule of thumb is to apply the norms and principles you would in person and to use common sense.

It is also important to be clear what support you can and cannot offer to participants online. Do not promise something that you aren’t qualified to deliver. If you are a practitioner rather than an arts therapist, for example, be clear to manage participants’ expectations about the depth of support you can offer. Clarity is key.

Advice for specific groups

There are many specialist resources available online. Some are listed below:

- **Children and young people**: Thinkuknow | NSPCC | SWGFL | saferinternet.org.uk | internetmatters.org | The 5 rights framework | Safe CIC
- **Young people and vulnerable adults**: Safe CIC
- **Creative facilitation for children and young people**: Noise Solution
- **Older people**: Age UK
- People with **learning difficulties**: Foundation for learning difficulties
- Do-it-yourself online safety guide, written with **victims of domestic abuse** and **stalking** in mind, but relevant and applicable for anyone.