Safeguarding and digital technologies in research activities.

The COVID-19 pandemic has had significant impacts on the lives of most people, and social interactions have become mediated much more through digital technologies than was heretofore the case. Digital technologies are usually promoted as having positive impacts, or at worst being benign. This, though, is an unrealistic picture, and their ability to accelerate and accentuate negative as well as positive behaviours and experiences gives rise to significant safeguarding concerns. While the term safeguarding is traditionally used to refer only to children and vulnerable adults, it is now used much more widely and in a sense everyone without good knowledge of how to use digital tech safely is subject to potential harm from its abuse. The relevant safeguarding issues can broadly be divided into those relating to the self, those relating to others, and those impacting the environment.

Taking care of oneself

Many people have experienced a considerable increase in the time they spend using digital technologies as a result of COVID-19, not all of which is healthy or indeed safe. Those responsible for safeguarding should always check that their staff enjoy the use of digital technologies safely, securely and wisely.

- *Time out*. Try to spend at least one day a week without use of any digital devices or connectivity; learn again the joys of the physical world, and the beauties of nature.
- *Digital duration*. How long do you spend using digital technologies each day? This can be very harmful both to the body and to the mind. Think about installing a screen-time checker that will let you know! Ensure your working environment (desk, screens, chairs) is appropriate for your body. Give your eyes some time to relax and explore distant horizons. Get up and take a short walk at least every hour.
- *Office hours*. Digital tech is frequently used to extend work time, and this has been exacerbated during COVID-19 lockdowns. Set yourself appropriate office hours, and don’t respond to e-mails out of these. Submit a formal complaint if your boss insists you respond to e-mails all hours of the day and night. When working across time zones always ask for arrangements to be made that can include you at appropriate times. Don’t self-exploit (unless you really want to).
- *Privacy*. The more time you spend on digital technologies, the more information you give to others about yourself. You might be happy to be merely a data point, but if not don’t just automatically click on accept when asked about permissions or cookies. Think about using software that limits how much others can find out about you. Use search engines that offer privacy such as DuckDuckGo.
- *Security*. Always install relevant protection (antivirus, web, ransomware, privacy, malicious traffic) and use it (techradar Guide). Create complex passwords. Be aware of scams, spam and phishing attacks, and keep safe by never simply clicking on links without checking that they are safe – especially if they are from people not know to you.

- *Online conferences and meetings*. Be very careful in online calls, especially if you cannot see everyone. In face-to-face meetings it is possible to pick up signs of how people react to what you are saying and thus adjust in real time, but this is impossible with most video calls. It is thus easy to cause offence without meaning to. Don't waste your time attending the thousands of online conferences or meetings that you are invited to - most are a complete waste of time. Only join ones that are critical to what you are doing, or are of real interest. Think of limiting your time to c. 8 hours of online meetings a week, and spend the rest doing things that are productive and worthwhile!
- *Use social media carefully*. Social media can be great for connecting with people that you want to, but it can also be deeply hurtful and the cause of much violence. Be careful over what you write, and avoid using it if you are angry or tired. If you are trolled, *never* reply because it only exacerbates the attacks. Don't just accept anyone as an online friend unless you know who they are. Take time away from social media. Read guides on wise use of social media (such as that produced by Greater Good at Berkeley). Report any abuse or harassment to the appropriate authorities (see how to respond to digital violence).
- *Never use personally identifiable media for professional purposes*. In particular, do not use your own digital media for research purposes. Instead, always ask to use official e-mails, telephone numbers and media outlets. For example, never use your personal mobile number to join a group on apps such as WhatsApp, especially for conducting interviews or focus groups, because you can never be sure who else is in the group, and what they might subsequently contact you about.
- *Behave wisely*. Remember that it is almost certain that some-one/thing, somewhere is almost certainly tracking and recording in some way everything you do online. Do not be the one who causes harm to others online.

Do to others as you would have them do to you - but remember they are different from you

In many ways, safeguarding advice relating to others is the application of the above principles to everyone else, but especially to members of the team of which you are a part, and all those with whom you are researching. It is crucially important to remember, though, that what is deemed to be acceptable use to some may not be acceptable to others. There is as yet little global agreement on what is acceptable behaviour in using digital technologies.

Within a team

General advice that is often seen as being helpful for avoiding digital harm includes:

- Always *listen* more than you speak in digital meetings – and do listen, rather than doing all the other digital things you need to catch up on;
- *Never impose one particular technology* on everyone in the team - try to reach consensus but if someone will not use one particular app or device, find an alternative solution;
- *Never expect an immediate response* to an e-mail, or on social media - if you wish to send e-mails at four in the morning your time do not expect others in your time-zone to respond*;*

- Dramatically *reduce the number of online meetings* that you think should be held, especially when working across time-zones – most are an excuse to pretend people are working, most are poorly managed, and it is much more efficient to seek input on policy documents by sharing drafts (if relevant using multi-authoring tools) than it is to do so in an online meeting;
- *Be accepting of varying cultural digital practices*, but make it clear if any of these offend you and explain why; and
- *Be strict in clamping down on any use of digital technologies for sexual harassment or other forms of abuse* – these should be reported immediately through standard existing safeguarding procedures;
- Find ways to *mitigate the personal costs* to team members of using digital technologies – remember that costs of internet connectivity, hardware and apps can be high for individuals, especially in economically poorer contexts;
- Always ensure that team members are *fully trained in how to use the digital technologies* chosen by the team, and are fully aware of protocols concerning security, safety and privacy;
- Ensure that all material and *data relating to the team's research activity is kept as digitally secure* as possible, encrypted on trustworthy servers, and with strong password protection;
- Always *explain if you are recording a meeting*, and do not do so if any team member objects – also, don't be critical of those who object for whatever reason.

With research participants

- Always explain to research participants *how you will use and protect any digital data* that you generate together;
- If you need participants to use any digital technologies, *ensure that they are fully trained in their use*;
- *Never force participants to use a specific piece of digital technology* (or app) – always try to use the technologies with which they are familiar;
- *Never use digital surveillance or tracking mechanisms* without the explicit and fully informed permission of participants – and even then try to find an alternative (you never know who else might be accessing the information);
- *Do all you can to protect participants from harm or abuse from their use of digital technologies*.

Think about the environmental impact of the digital technologies you are using, and mitigate their harms

Digital technologies are often seen as a good way to reduce environment harm, but this is by no means always so, and many practices in the digital technology sector are anti-sustainable (see further here). Those who consider that environmental harm should be included within safeguarding should be aware of the following:

- The *ICT sector contributes more carbon to the atmosphere than does the airline industry* (see here from 2017) – virtual conferences are not carbon-neutral;
- *Video uses much more bandwidth and electricity than does audio* (see here) – encourage participants in online meetings to keep their video off when they are not speaking;

- *Never contribute to e-waste by purchasing new digital tech just for the sake of the research grant* – do all you can to repair and reuse your digital tech, and only purchase new when you absolutely have to (see the The Restart Project for examples and evidence);
- *Use digital tech* (both hardware and software) that is as environmentally sustainable as possible;
- *Minimise the use of electricity* (including in data servers, device production, and device usage), and where possible use renewable powered energy (such as solar mobile devices);
- Purchase and use digital tech (including apps) from *companies that are committed to minimal environmental impact* (not just satisfying carbon emissions criteria);
- Always switch off digital tech when not in use, and don't just put them on standby;
- Consider conducting an environmental audit of all digital tech used in your research.

Version 2
4th June 2021