WHY IT IS IMPORTANT

Social media and related risks

Social Media (like Facebook, Twitter, YouTube, TikTok, Blogs or relaying Digital Images online) pose opportunities and serious risks to Participants, Teams, Team Members and Organisations including:

- Participants viewing inappropriate personal material on a Team Member's personal site.
- Participants defaming other participants.
- Cyber bullying.
- Breaching privacy laws, through images being displayed without permission.
- Cyber predatory behaviour.

Helping teams and participants manage safety online

We cannot control the way team members and participants use the internet and social networks. We can, however, bring awareness of the issues to both team members and participants, and provide guidelines for safety management in this area. While there are strict privacy legislation guidelines regarding the use of information and images for organisational activities and publications, the ease of access to sites and problems that can arise usually mean people are chasing an issue or problem rather than being ahead of it.

And this is not simply a risk to younger people, but to adults as well who are duped by misrepresentation or cyber fraud in an effort to defraud or compromise people's personal information or image for improper and financial gain.

WHAT WE NEED TO KNOW

To provide the best possible care for children and young people, organisational staff, volunteers and organisations must mitigate risks from content, conduct and contact on social media and other digital platforms.

Friends and 'friending' on sites

- Do not request that minors (those under the age of 18) become your friends on your personal social networking sites, given your leadership role.
- A good code of conduct suggests all leaders (including team leaders) who have participants in the organisation's events as friends on their personal site, would declare this early, as a transparent approach.
- This is to clearly separate your 'professional relationships' from personal ones, thus avoiding conflation that can be used as a cover to manipulate for malicious intent.

Content on sites

- Remember that people connected to your profile, have the ability to download and share your information with others. This includes posts, photos and videos.
- Decide whether a particular post, photo or video puts your effectiveness as a team member or your organisation at risk.
- Post only what you would be willing for the world to see. Imagine participants, their parents, team leaders, and your organisations' representatives visiting your site.
- Posting to social media is not the same as posting something to your web site or blog and then realising that a story or photo should be taken down. Once it is on Facebook, Twitter, Tik-Tok and many more, it cannot be retrieved. It is effectively a public domain.
- Do not criticise team members, participants, or your organisation on social networking sites.
- Do not post images or videos that include minors on any site. Team members should only converse with minors via wall posts and not through one-to-one chats (e.g. Messenger or Snapchat). If conversation is initiated by a

minor, keep the conversation transparent – only communicate what their parents would be happy to read and suggest this is not a sustained way to make contact.

Team authorised social media pages

- The team should have two separate pages/sites – one for team members (leaders) only and one for participants and team members.
- Team leaders or other senior team members should be administrators of both pages/sites and monitor them on a regular basis.
- Pages on both sites should be set to the highest level of privacy, and all content should only be visible to members and participants respectively.
- Only current team members, and participants should be accepted as members/friends on the participant's page. Past team members can be friends on a team only page.
- Photos and videos of participants should not be posted to sites/ pages by team members without their authorised consent or that of their caregiver.

Guidelines for participants

- Brief participants at the end of the program, with the same guidelines – they should get permission from people in the photos before posting them.
- Encourage team members and participants to write only encouraging things on sites like Facebook and Twitter and to avoid the potential for defamation which could result in legal action.
- Address the issue of cyber bullying proactively and firmly.

WHAT WE NEED TO DO

Action plan

- Discuss these issues with your team and be vigilant.
- Audit your team sites.
- Invite the team to participate in discussion about how you might help participants to adopt responsible behaviour on-line.
- Ask teams to invite participants to share any online actions they consider to be scary, unsafe, or suspicious, with a view to enabling their feedback, experiences and concerns.
- Ensure young participants know who to contact if they experience online problems.
- Develop a 'permission to use' (images) protocol for your organisation.
- Ensure parent or guardian prior approval is given for both child participation in any Social Media and any use of images of child participants
- The organisation should have two approved and designated leaders monitor and moderate organisation Social Media accounts to provide transparency.
- Live video sessions that include child participants should be password protected to preserve the child's privacy and protect from any third-party inappropriate content (also see CSE4-OLS Livestreaming safety checklist).

Useful References

https://www.esafety.gov.au/young-people
https://www.esafety.gov.au/kids/i-want-help-with
https://aifs.gov.au/cfca/publications/online-safety
nspcc.org.uk/keeping-children-safe/online-safety
https://www.gov.uk/government/publications/child-safety-online-a-practical-guide-for-providers-of-social-media-and-interactive-services/child-safety-online-a-practical-guide-for-providers-of-social-media-and-interactive-services
https://www.netsafe.org.nz/
https://10play.com.au/mirror-mirror a 2-part documentary on serious online risks
Megele, C. (2017). Safeguarding children and young people online: a guide for practitioners. Policy Press. Bristol, UK