Managing Safety in Social Media

Why it's important

Social media and related risks

Social Media (like Facebook, Twitter, YouTube, SMS, Blogs or relaying Digital Images online) poses new risks to 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 predator behaviour leading to serious crime

Helping teams and participants manage safety online

We cannot control the way Team Members and participants use the internet and social networking tools. We can, however, bring awareness of the issues to both Team Members and participants, and provide guidelines for Safety Management in this area. There are strict Privacy Legislation guidelines regarding the use of information and images for organisational activities and publications.

What I need to know

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.
- You must advise your Team Leader which participants are friends on your personal site (just as you would advise them who you are keeping in contact with).

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 want 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 or Twitter, 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. They can do this for themselves. Team members should only converse with minors via wall posts and not through one to one chats (e.g. MSN or Chat). If conversation is initiated by a minor, keep the conversation transparent – only communicate what their parents would be happy to read.

Team authorised social media pages

- The team should have two separate pages/sites – one for team members 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 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 I need to know

Action plan

- Discuss this with your team
- Audit your team sites
- Invite the team to participate in discussion about how you might help participants to adopt responsible behaviour on-line
- Be vigilant on what is posted on the team site
- Develop a 'permission to use' (images) protocol for your organisation

What I need to do