Activity Alliance
E-Safety Policy

activity alliance
disability inclusion sport

activityalliance.org.uk

Contents

Introduction and terms 3

Activity Alliance e-safety checklist 3

Do's and don'ts 4

General good practice 5

Text messages (SMS) 5

Instant messaging service 5

Emails 5

Version:	2	**Reason:**	Update
Approved by:	Activity Alliance Board	**Approved date:**	**April 2018**
Review date:	Jan 21	**Reviewer:**	Safeguarding lead

If you require this document in a different format please contact Info@activityalliance.co.uk

Introduction and terms

This policy provides guidance on the procedures that will support and underpin the use of social networking and other online services within Activity Alliance. It is important that all staff, volunteers, board/trustees and federation members, or anyone working on behalf of the organisation are aware of this policy and agree to the following terms:

Terms:

- To protect all children, young people and adults at risk associated with activity alliance activities and those who make use of technology (such as mobile phones, tablets, games consoles/hand held devices and the internet) whilst they are in the care of activity alliance.

- To provide staff and volunteers with policy and procedures information regarding e-safety

- To ensure everyone associated with activity alliance is operating in line with our values and within the law regarding how activity alliance uses information technology.

Activity Alliance e-safety checklist

1. All staff and volunteers understand the safety aspects including what is acceptable and unacceptable behaviour when using digital technology such as social networking sites (e.g. Twitter and Facebook), mobile phones, tablets, games consoles and the internet.

2. When engaging with digital technology/social networking companies (e.g. Facebook, Twitter etc.) it is important to ensure that everyone associated with activity alliance adheres to relevant legislation and good practice guidelines.

3. activity alliance regularly reviews existing safeguarding policies and procedures to ensure that online safeguarding issues are fully integrated.

4. activity alliance digital communications will be managed as follows:
    a. Vetting and managing the webpage/profile
    b. Training for person/s managing the organisation's online profile
    c. Involvement of the activity alliance safeguarding lead officer where needed
    d. Ensure that any interactive content is moderated

5. Ensure that adequate privacy settings are in place either restricting or allowing access to photos, personal information, comments about others, friends and followers.

6. Ensure that staff and volunteers are aware of the need to protect their privacy online. Staff and volunteers are encouraged to carefully consider who they give access to their personnel information to online. activity alliance ensures that there is a clear differentiation between personal and professional profiles. For example, we ask staff to add in the copy within their personal Twitter pages that their tweets are their own view

7. Always address safeguarding when promoting activity alliance and its supporting partners.

Do's and don'ts

Do

1. Set your privacy settings for any social networking site to ensure only the people you want to have sight/access to the contents. Keep these updated. The default settings for most social networking sites are set to open access where anyone can see everything.
2. Ensure your mobile phone (any technological equipment) is password/PIN protected. This will ensure that other people cannot use your equipment and get you into trouble.
3. Consider having separate personal and professional online identities/accounts if you wish to have online contact with service users i.e. children/young people/adult participants, their families and other professionals. Ensure that your manager is aware of your professional online persona.
4. Make sure that all information about you that is publically available is accurate and appropriate – think particularly about whether photographs/stories that you may have posted in your personal life are appropriate for a person with a professional life and a reputation to lose. If you do not want it to be public, do not put it online.
5. Remember that online conversation may be referred to as 'chat' but they are written documents and should always be treated as such. Be mindful about how you present yourself when you are publishing information about yourself or having 'conversations' online.
6. Make sure that you are aware of your organisations policy regarding the use of both organisational and personal digital equipment and the consequence of misuse. Breach of the policy can result in capability/disciplinary actions by your employer, professional body and criminal proceedings by the police.
7. Act on the side of caution. If you are unsure who can view online material, assume that it is publicly available. Remember – once information is online you have relinquished control of it. Other people may choose to copy it, to edit it, to pass it on and to save it.
8. Switch off any Bluetooth capability any device may have installed as standard. Bluetooth allows another person to have access to your personal equipment – they can then pretend to be you.
9. Always be aware that technology is constantly upgrading and improving. You may have access to websites via a work-provided smart phone that are blocked by your computer. Mobile phones come with locator software. Cameras can be a feature of games consoles. When you receive any new equipment (personal or private) make sure that you know what features it has as standard and take appropriate action to disable/protect.

Do not

1. Give your personal information to service users i.e. children/young people/adult participants, their parents /carers. This includes personal mobile phone numbers, social networking accounts, personal website / blog URLs, online image storage sites, passwords / PIN numbers etc.
2. Use your personal mobile phone to communicate with service users i.e. children/young people/adult participants, their parents /carers either by phone call, text, email or social networking sites.
3. Use the internet or web-based communication to send personal messages to service users i.e. children/young people/adult participants, their parents /carers/personal assistants, that are not work related.
4. Share your personal details on a social network site with service users i.e. children/young people/adult participants, their parents /carers. This includes accepting them as friends. Be aware

that belonging to a 'group' may give 'back door' access to your page even though you have set your privacy settings to family and friends only.

5. Add/allow service users i.e. children/young people/adult participants, their parents /carers to join your contacts/friends list on personal social networking profiles.
6. Use your own digital camera/video for work. This includes integral cameras on mobile phones. Unless given permission by the communications or safeguarding team.
7. Play online games with service users i.e. children/young people/adult participants, their parents /carers. This can be difficult when the culture is to play strangers. Check out before you play online with someone you do not know.

General good practice

It is inappropriate for adult staff and volunteers to communicate on a **one to one** basis directly with service users- children/young People/adult Participants by:

- Text message
- Email
- Instant messaging
- Through social networking sites

All digital communication by the above methods should include (where possible) a copy to a third party, e.g. copy to relevant safeguarding officer and/or parent. Where social media sites do not allow a third party copy, you should keep the communication on the site and inform the safeguarding officer of the conversation.

Text messages (SMS)

Text messages are not the preferred method of communication between adults and service users i.e. children/young people/adult participants. Given that we work with many audience groups who use text for an accessible communication (eg. deaf people), we should be aware that where they are used for other communication reasons, they should be group messages, then should be copied into the relevant safeguarding officer and/or parent.

In the event of an emergency, individual texts may be used but again must be copied into the relevant safeguarding officer and/or parent.

Instant messaging service

MSN, Yahoo, Whatsapp and other instant messaging systems should not be used by adults to communicate with service users i.e. children/young people/adult participants under any circumstances.

Emails

Emails are a positive and simple method of communication between adults and service users i.e. children/young people/adult participants and groups are easy to set up.

Group emails are preferred, although in the case if an email to one person, a copy must be sent to the relevant safeguarding officer and/or parent.

For more information, please contact info@activityalliance.org.uk or call 01509 227750

www.activitylliance.org.uk