



E-Safety Policy

[Italicised words are defined in the glossary at the end of this document]

Purpose

We need to ensure that Allsorts is using digital and *social media* in safe, appropriate, inclusive and creative ways.

Scope

Service-users, trustees, paid staff and volunteers, technical advisors and digital visitors - all who are using *digital social media* at or via Allsorts are subject to the guidance provided in this policy.

Authority

This document has been adopted by the Allsorts Board of Trustees/Management Committee.

What digital and social media do Allsorts use?

Facebook:

- *Profile page* called **Allsorts Staff**
- *Like page* called **Allsorts Youth Project – Supporting LGBTU Youth and Transformers – Trans Youth Brighton**
- *Group(s) on Facebook*, called **Transformers – Brighton Trans Youth Network, Allsorts Peer Educators, No Dress Code – young women’s group, TAG LGBTU Group (13-15 y/s old), Young People’s Voice @ Allsorts, Male Matters GBTU young men’s group**

Twitter: Our username (*profile page*) is **@AllsortsYouth**

YouTube: Our *profile page* is called **‘Allsorts Youth Project’**

Tumblr: Our blog link is **transformersyouthproject.tumblr.com**

Website: **www.allsortsyouth.org.uk**

Digital and social media use for trustees, paid staff & volunteers

1.1. Basic Principles

Trustees, paid staff and volunteers must keep a professional distance online, just as they would in the offline world. Compared with a conversation in the offline *real* world,



technology increases the potential for messages to be taken out of context, misinterpreted or forwarded to others.

Trustees, paid staff and volunteers must bear in mind that once they place something in the public domain, it is there permanently for people to access, change and share it with others.

The key principles in *digital* and *social media* use are the same as in any professional interaction:

- Trustees, paid staff and volunteers working with service-users should reflect the positive messages they give service-users through their public behaviour
- Trustees, paid staff and volunteers must be clear about where the boundaries are in the support they offer to service-users, and must avoid setting up false expectations
- Trustees, paid staff and volunteers must ensure they are not put in the position of having to deal with information or situations that they are not confident or comfortable to deal with
- Allsorts must ensure that they do not create situations in which trustees, paid staff and volunteers could cause harm to service-users
- Any *moderators* or *administrators* whether trustees or staff with permitted unsupervised access to service-users through *Social Network Sites(SNS)* must be DBS checked
- Trustees, paid staff and volunteers working with service-users must not use their personal social networking account to communicate with service-users

1.2. General policies and procedures

- **Service-users who become trustees, paid staff or volunteers:** Allsorts, as a peer led organisation, recognises that some trustees, paid staff and volunteers are now (young people trustees) or have been service-users in the past or, as young people, fall within the age range of service-users. It is unreasonable to expect them to cut their personal social networks with their friends who may still be service-users. However, this creates potential risk.

If trustees, paid staff and volunteers have their own personal *SNS profile*, they must ensure that service-users cannot access any content, media or information from that *profile page* that relates to Allsorts or which would undermine their position as a professional, trusted and responsible adult working or volunteering with service-users at Allsorts either as trustees, paid staff and volunteers.

Trustees, paid staff and volunteers who are currently or who have been service-users must moderate their use of SNS to reflect their status at Allsorts accordingly just as



they would moderate their behaviour in the offline world to reflect their responsible, role modelling status.

- **Other trustees, paid staff and volunteers:** All other trustees, paid staff and volunteers who use their own personal *SNS* must ensure that service-users from Allsorts cannot access any content, media or information from their personal *profile page*. Trustees, paid staff and volunteers must check their privacy settings regularly to ensure this.
- Only Allsorts official pages, profiles, groups and sites can be used to share information relating to Allsorts. This boundary must not be confused by the use of personal *SNS* to convey information about Allsorts by any trustees, paid staff and volunteers. For example, do not message service-users from your personal Facebook profile as this will blur boundaries between your professional and personal lives.
- Trustees, paid staff and volunteers must review regularly that they have no '*Friend*' connections on their personal *SNS profile* with the service-users they work with. You should not accept '*Friend*' requests from service-users you work with to your personal *profile page(s)*. Paid staff and trustees who have been or are currently service-users are exempt from this clause.
- When entering into social media discussions outside work where a trustee, paid staff or volunteer might be seen to be representing Allsorts when in fact they are speaking as a private individual, they must make this clear with an explicit statement to this effect.
- Staff may only set up pages for events, activities or groups for which they are responsible and have '*officer*' or '*admin*' responsibilities for. The staff member with key responsibility in any context must always be the *administrator* or *officer* of these spaces.
- If, on behalf of Allsorts, you create a *group*, host *discussions* or encourage *media-sharing*, then the *Moderation Rules* (in Section 6) must be adopted. These provide rules for service-user engagement. You must create a group agreement with these ground rules about the kind of language, *discussions* and *media sharing* allowed. Make sure these guidelines are created with service-users in mind and are accessible.
- Even with stringent *privacy settings*, the nature of *social networking sites* like *Facebook*, means it is difficult to avoid seeing content from service-users which a trustee, worker, or volunteer may not wish to see/should not see outside their paid/voluntary role. Trustees, paid staff and volunteers must not post or comment on the status, wall or photos of any service-users. Trustees, paid staff and volunteers who have been or are currently service-users are exempt from this clause but their comments must nevertheless reflect their responsible and role modelling status at Allsorts.
- Trustees, paid staff and volunteers engaged in promotional or campaigning activities for Allsorts will be encouraged and offered support to make maximum use of digital



and social media as part of their work.

- Trustees, paid staff and volunteers must not bring the organisation into disrepute in their use of digital and social media.

1.3 Specific protective guidelines for trustees, paid staff and volunteers

- You must ensure you have clear understanding on who to contact if you have any concerns about service-users safety online. Use the same chain of authority and advice (e.g. Director and Chair) as used in the generic Safeguarding Policy. If in doubt, go up a management level and consult.
- In all contexts, you must conduct yourself in an appropriate way as you would face to face - be hyper aware of what you say and how you say it.
- Be mindful that even if you delete a comment straight away, someone might have already seen it. SNS sites happen in real time and some service-users are often constantly online and will see things as they happen.
- You must not provide personal details about service-users on the website, SNS or *social networking group* (this includes full name, email address, etc).
- You must ensure that you have permission to use any photos of service-users and only use their first names on any caption. *Tagging* of service-users in photos/videos will remain the responsibility of the individuals themselves and not trustees, paid staff or volunteers.
- Only use appropriate photos, the sort that you would be happy putting on a public notice board - remember that everyone can view them.
- If you have one-to-one contact with a service-user using *chat/instant messaging* and provide *e-mentoring*, the conversation must be copied into a Word document and printed off. It must be attached and recorded on the Allsorts one-to-one monitoring form.
- If you would like to use a quote from a service-user which has been said during one-to-one contact, you must ask permission before you use it and clarify how the young person wants the quote attributed.
- If you are concerned about the way a service-user is attempting to contact you, report it immediately to your line-manager.
- The Director and trustee lead for digital and social media have overall responsibility for monitoring social media interaction on *Timelines, discussions boards, blogs, comments on photos/videos, tagging of pictures/videos* and '*Group*' or '*Fan Pages*' and *Twitter* mentions.
- Ensure you do not infringe copyright. If you use photos taken by someone who is not part Allsorts, then ensure you credit the images. The same practice applies for any other content that has not been created originally by Allsorts.
- Allsorts intellectual property rights and copyright must be asserted when publishing online
- Service-users in leadership roles, especially involving campaigning, need independent access to Twitter and permission to tweet, re-tweet or reply to posts.



Service-user leaders' access will be monitored and reviewed on a regular basis. If it is misused, it will be revoked.

2. Passwords

Staff must keep Allsorts account and password details in a safe place. They must be changed every two months in order to make them more secure. They must ensure that the Director and trustee lead for digital and social media have overall access to e-mail accounts and networking sites for when they are on leave, absent or no longer working with the project. When staff leave the project, passwords must be changed.

3. Email & SMS (texts)

- Emails sent to external organisations should be written carefully in the same way as a letter written on Allsorts headed paper.
- Emails to a service-user must be printed off and filed with a one-to-one form. This email should then be deleted both in your inbox and the Sent file for data protection.
- When sending emails to groups of service-users, staff must use the 'BCC' facility to avoid sharing e-mail addresses.
- Staff may only use Allsorts e-mail accounts to contact service-users.
- Staff must not reveal personal details of themselves or others in e-mail and SMS communication, or arrange to meet anyone without specific permission.
- If a text is sent to a service-user, it must be sent from an official work mobile.

4. Publishing service-users' images and creative work

- At induction, service-users will be informed that if they would *not* like to be used in Allsorts publicity, that they must make themselves known to staff at the time of photographing/videoing. When images/videos are posted of service-users, no names should be mentioned and no-one should be tagged.
- Service-users full names will not be used anywhere on the website or SNS, particularly in association with photographs and videos. *Tagging* of service-users in photos/videos will remain the responsibility of the individuals themselves.
- At induction, service-users will be informed that if they would not like to have their work used in publicity, that they must make it known at the time their work is gathered by an Allsorts member of staff.



5. Staff use of the hardware, digital and social media at work

- Staff may only use the PCs/laptops for personal use during lunch times or by arrangement.
- Staff may not use email or social media for unofficial or inappropriate purposes, including:
 - any messages that could constitute bullying, harassment or have any other detrimental impact, as well as *Flaming* (deliberately provocative communications)
 - on-line gambling
 - accessing or transmitting pornography
 - transmitting copyright information and/or any software available to the user
 - posting confidential information about other employees, the company or its customers or suppliers
 - contact with extremist groups or political parties
- The use of digital and social media at work using Allsorts equipment and internet connections to access and/or distribute any kind of offensive material, inappropriate sites considered pornographic or those of extremist organisations e.g. BNP or political parties will lead to disciplinary action.

6. Moderation rules

Allsorts will delete any of the following:

- Violent, obscene, profane, hateful, or racist posts, links or images
- Comments that threaten or defame any person or organisation
- Solicitations, advertisements, or endorsements of any financial, commercial, political party or not-for-profit organisation
- Comments that suggest or encourage illegal activity
- Multiple successive off-topic posts by a single user
- Repetitive posts copied and pasted or duplicated by single or multiple users

7. E-safety complaints procedure

- Complaints of internet misuse will be dealt with by the Director and/or Chair;
- Any complaint about staff misuse must be referred to the Director and/or Chair.

8. E-Safety for service-users



Many service-users assume they are safe when using the internet because they are in their own home or in another safe place. They will usually assume that the person they are chatting with is who they say they are and have harmless intentions. Most of the time, this is true.

However, service-users accessing social and digital media need information about ways in which they can use these platforms safely, understand the risks in the online environment and protect themselves. This is even more important now that the internet is available on SMART phones.

The following E-Safety briefing provides basic advice to service-users. It must be distributed and explained on a regular basis to service-users attending services provided by Allsorts:

Tips to Be Safe Online

- **Never give out personal information to online friends. This includes an instant messaging ID, email address, mobile number, school name and any pictures of you, your family and friends**
- **If something is published online, anyone can access it, change it or share it with others. Keep social network profiles private**
- **Use webcams with caution and only with family and friends who are already known in the real world, as images can be copied, changed and shared**
- **Do not post inappropriate images of yourself online**
- **Remember that *online friends* are just that and if they are not known to you in the real world, offline, they may be lying about who they are**
- **Never meet up with a person you have met online unless you take a trusted adult with you**
- **Think before opening files from people you do not know in the offline *real* world. They may contain anything from a virus to an inappropriate image or film and should be deleted**
- **Learn how to block someone online and report them to the website involved. Report abusive users to the Child Exploitation and Online Protection Centre (CEOP) if you feel uncomfortable or threatened. Save the www.clickceop.net website to your favourites so that you can report any suspicious behaviour straight away**



- **Online location tools, such as *Facebook Places*, should not be used by those who are under-18 or if you are in a location alone.**

9. Use of computer room/IT suite at Allsorts

- Service-users must use the PCs and laptops with care and consideration of their value and fragility.
- They must report any faults or viruses immediately.
- They must not use the internet to view or engage in activities that would cause offense and would compromise Allsorts as a safe space e.g. sites that contain violence, sexual or extremist content.
- Service-users must be willing to show the web-page which they are viewing at any time to a member of staff or volunteer. Refusal results in an immediate request to leave the computer room/IT suite.

E-Policy Glossary

- **Admin/Officer** – This is the individual who has overall responsibility for the group or fan page on Facebook. This is usually the creator of the group/fan page, but individual can also be designated admin/officer status by another member with admin/officer status.
- **Blog** – Contraction of the term ‘web log’, a blog is a form of online journal with articles posted on particular subjects. **WordPress** is one of the most popular blog creation websites.
- **Discussions** – These take place on a *Discussion Board* and are the same as a *Forum*. As an *Admin/Officer*, you can start a new *thread* which is a question or statement. People are then able to respond to the question or statement.
- **Discussion Board** - same as a *Forum* whereby people exchange opinions and advice or answer questions based on a *thread*.
- **E-mentoring** - a means of providing a guided mentoring/support relationship using online tools such as *Instant Messaging (IM)* or email.
- **Facebook** – The web’s most popular *social network site (SNS)* which allows users to present an online ‘*profile*’, form online groups and *media-share*.
- **Facebook Fan Page** – a public profile used by charities, organisations, businesses, celebrities or public figures. It allows you to share information with individuals or other organisations that are supporters of your aims/objectives and have ‘**liked**’ your page. As well as posting up information into your status, you can ‘share’ information to your supporters from other relevant organisations.
- **Facebook Group** – You can create a group from your **Profile Page**. Groups allow individuals who are Facebook members and have a Profile Page to join. Groups can be



closed and private where only you as creator can invite people to join, or the group can be open and public, where anyone can join and see the information being shared amongst members. From your group you can use the Facebook email to contact all the people who have joined the group.

- **Flaming** – insulting someone to provoke a negative reaction.
- **Forum** – same as a *Discussion Board* whereby people exchange opinions and advice or answer questions based on a *thread*.
- **Facebook Places** – an on-line tool that tells people your precise location – linked to your **Twitter** and/or **Facebook Timeline/Wall**. People often use this to tell followers and friends the venue or event they are at.
- **Instant messaging (IM)** - A type of communication where two people communicate privately in [real time](#) over the [Internet](#), like a telephone conversation but using [text](#)-based, not voice-based communication.
- **Media-Sharing** – a term used to describe the exchange of photos, videos and links online between individuals and organisations.
- **Moderator (at Allsorts)** – This is the individual, in this case the Administrative Manager, who has overarching responsibility for monitoring on-line activity of **SNS** on behalf of the organisation. This person posts information about Allsorts activities or that of other organisations and media, ensures that comments are appropriate and responded to, alerts staff of contact by service-users either through **SNS** email, **instant chat** or comments and ensures that the **profile page** and **fan page** are up to date.
- **Moderation Rules** - guidelines or rules for those you are engaging with in an on-line public space such as a group. This can include the sorts of language, *discussions* and *media sharing* allowed. Please see an example of Moderation Rules in Section 6.
- **Privacy Settings** – These allow you to put restrictions on who can see the information on your *SNS Profile Page*. It also allows you to restrict how and with whom information about you is shared publicly.
- **Profile Page** – This is your **SNS** individual profile and is your launch pad for using other SNS tools on the site. Staff need to create an individual work profile page so they do not have to use their private profile page to communicate with service-users. Your Profile page can be made the ‘**administrator**’ or ‘**officer**’ of a **fan page** or **group**.
- **SNS/ Social Networking Site(s)** - on-line tools that allow people and/or organisations to connect together for example **Twitter, Facebook, YouTube**.
- **Social Marketing** – using on-line tools to promote and raise awareness of your company for a specific objective.
- **Social Media** – an umbrella term for any on-line tool or phone application (*app*) which allows an individual or organisation to communicate with their service users and supporters. It also allows its users to enter a dialogue with each other. This can be through sharing of images or videos, sending messages to one another or writing articles which other users can alter or post comments on.
- **Social Networking** – on-line tools that allow people and/or organisations to connect together.
- **Status update** – 450 characters on Facebook and 140 characters on Twitter in length,



this is the exchange of comments, information and links from your *Profile Page* to the *wall* of those you are linked to as 'Friends' or 'Fans' or 'Followers'.

- **Tagging** – this is when people are identified in *media-sharing*. Individuals can tag themselves or be tagged by friends and/or the admin/officer of a group/Fan page.
- **Thread** – A topic of discussion taking place on a *Discussion Board* or *Forum*. A thread begins as a question or statement and is continued with an exchange of comments/responses.
- **Timeline/Wall** - A space provided with your *Profile Page* or *fan/like page* to share messages, opinions, and links to those you are connected with as 'Friends' or 'Fans'.
- **Twitter** – Micro-blogging service which allows users to provide 140-character updates. Users can 'follow' each other but unlike other social networks, it is not automatically reciprocal. Twitter allows you to 'follow' a great many people/organisations who will be communicating about specific subjects regularly and as such is a good way of getting the latest information specific to your interest.
- **YouTube** – Video-sharing network which allows users to upload and share video footage with others. 'Links' to these videos are then easily sharable through other mediums and platforms.
- **Wall/Timeline** – A space provided with your *Profile Page* or *fan/like page* to share messages, opinions, and links to those you are connected with as 'Friends' or 'Fans'.
- **Wiki** – For example **Wikipedia**, allows users to create, edit and link web pages easily; often used to create collaborative websites (called '*wikis*') and to power community websites.

Acknowledgments

Allsorts would like to thank Jess Wood, Director, and Mel Berry, former Administrative Manager for updating this policy. We would also like to thank members of the Community & Voluntary Sector Forum (CVSF) Safety Net, B&H city council, and <http://network.youthworkonline.org.uk> who provided us with examples and information on e-safety and helped us to bring this document to a final draft.

We would like to thank specifically the following individuals: Susan Luxford, who wrote the original document, Adam Muirhead of the Trust for Developing Communities, Duncan Hill at the 15th Brighton Scout Group and Tim Davies of Youth Work Online.