2021/22

Social Media Policy

Clean Slate Policies

SOCIAL MEDIA POLICY

CONTENTS

1. PURPOSE

This policy outlines the use of social media applications, work-related and personal, by members of the workforce. The aim is to balance the communication and engagement opportunities that social media provides with safeguarding, legal and reputational concerns.

2. AUDIENCE

This policy is intended for all members of the workforce.

3. DEFINITIONS

For the purposes of this policy, the following definitions apply:

3.1 The Organisation

For the purposes of this policy 'the organisation' refers to Clean Slate

3.2 Social Media

Any web-based tools and applications which enable users to create and share content (words, images and video content), and network with each other through the sharing of information, opinions, knowledge and common interests. Examples include Facebook, Twitter, LinkedIn and Instagram.

4. ORGANISATIONAL SOCIAL MEDIA

4.1 What to Do

When using **the organisations** social media, members of the workforce shall:

- share great ideas and spread the message about the fantastic work the organisation does.
- use the organisations branding elements (e.g. logo).
- check the privacy settings and be mindful that content may be shared beyond their network once posted on social media.
- be aware that T&Cs and privacy settings may change so should be periodically checked.
- obtain approval from a responsible manager or the CEO to create any new social media accounts under the organisations name.
- obtain permission if a post includes or relates to a particular individual.
- adhere to the organisations code of conduct.
- advise the CEO before taking any action if approached by a media contact about any social media post/content.

4.2 What NOT to Do

When using **the organisations** social media, members of the workforce shall not:

- publish any content which may result in actions for defamation, discrimination, breaches of copyright, data protection or other claims for damages. This includes but is not limited to material of an illegal, sexual or offensive nature that may bring the organisation into disrepute.
- publish any content that can be perceived in an abusive or hateful manner.
- promote party political purposes or specific campaigning purposes not approved by the board.
- promote personal financial interests, commercial ventures, or personal campaigns.
- breach any organisational policy or procedure. This includes misconduct, equal opportunities, safeguarding, harassment, confidentiality, and data protection policy.

5. PERSONAL SOCIAL MEDIA

5.1 What to Do

When using **personal** social media, members of the workforce shall:

- access social media in their own time (e.g. lunch or coffee breaks) and not during work time.
- check their privacy settings and be mindful that content may be shared beyond their network once posted on social media.
- be aware that T&Cs and privacy settings may change so should be periodically checked.
- obtain permission if a post includes or relates to a particular individual.
- make it clear that the opinions expressed on social media are solely those of the user and do not represent the views of the organisation, if they are known to be or can be identified as a representative of the organisation.
- adhere to the organisations code of conduct.

5.2 What NOT to Do

When using **personal** social media, members of the workforce shall not:

- publish any content which may result in actions for defamation, discrimination, breaches of copyright, data protection or other claims for damages. This includes but is not limited to material of an illegal, sexual or offensive nature that may bring the organisation into disrepute.
- publish any content that can be perceived in an abusive or hateful manner.
- breach any organisational policy or procedure. This includes misconduct, equal opportunities, safeguarding, harassment, confidentiality, and data protection policy.
- use the organisations branding elements (e.g. logo).

- use the organisations computer/tablet/phone to access personal accounts.
- have current or past service users (or their family and/or friends) as connections.

6. BREACH OF POLICY

Any breach of this policy could result in the offending content being removed and the individual being subject to the organisations disciplinary procedures including dismissal.

7. FAQS

7.1 How does the organisation use social media?

The organisation use social media to share news about the organisation, as well as to engage with colleagues in the sector, partners and clients.

We aim to be open and transparent and to actively encourage the community to engage in conversations online.

7.2 Will I be able to use social media in work time?

You can only use social media in work time if you are authorised.

7.3 What information about the organisation can I share online?

You can share anything about the organisation that would be available to the public.

Any information that would be considered confidential (in line with the Confidentiality, Data Protection & Sharing Information policy) or protected by the Data Protection Act should not be shared. If you are not sure if something is confidential, don't share it.

If you are unsure about posting anything online, it's always best to stop and have a think first, or check with your line manager. If in doubt, don't share the post.

7.4 What do I need to do if I'm contacted by a service user through social media?

You should be pleasant and civil if approached, but discourage prolonged social contact and advise the service user of the appropriate channels of communication. This also applies to 'encounters' on social media sites.

If contact continues, you should escalate this to your line manager and refer to the organisations harassment policy.

7.5 Can I use my personal account to interact with the organisations social media?

We encourage you to engage with the organisation online, get involved in conversations and like and share our information.
However, you should not use your personal social media to speak on behalf of the organisation.

7.6 Can I say what I like online outside of work on a personal account?

You are responsible for what you say on the internet at any time of the day or night. While you are not acting on behalf of the organisation, you must be aware that you are obliged to act in accordance with the principles outlined in section 5 of this policy.

Never think that updates or online posts will remain as private as you might want –anything that is posted, whether on a personal account or not, can be shared and seen by others, whether intended by you or not. For example, if you post a comment on a friend's wall, their privacy setting will apply to your post so you won't always be able to control who sees what, so be very careful. Also, screenshots can be taken and shared, breaching these privacy settings.

If you make a mistake that may be in breach of this policy, notify your line manager immediately of what has happened.

7.7 Will my personal social media account be monitored by the organisation?

No. However you should exercise good judgement when posting things online and to be familiar with your privacy settings. Remember your audience could be anyone who uses the internet, so think about what you are saying.

Social media is a public platform and it is likely that a colleague or service user could come across your posts online even if your profile is private. Equally, if you see something that concerns you online, please let your line manager know straight away.

8. APPENDIX A –SERVICE USERS USING SOCIAL MEDIA

The following may be raised with service users to consider when using social media:

- Social media is a public platform so content (from any time) could be accessed by anyone who uses the internet. Even if a profile is private the posts may be shared beyond its network once posted on social media.
- Be aware that T&Cs and privacy settings may change so should be periodically checked.
- Consider turning off location setting on devices.
- Consider updating security settings such as password, secret question, linked email accounts.
- Be aware of tools to help safety online, such as the ability to report comments or block users.

The following links may be useful to share:

- https://www.womensaid.org.uk/wp-content/uploads/2015/11/Womens-Aid-Facebook-Safety-Guide-2017.pdf
- Facebook – security and privacy of Facebook Profile
- Twitter- security and privacy of Twitter
- Instagram – security and privacy of Instagram Profile
- LinkedIn – security and privacy of LinkedIn Profile
- Snapchat – security and privacy of Snapchat Profile
- YouTube – security and privacy of Youtube

9. VERSION HISTORY

It is recommended that this document is reviewed at minimum every 3 years. However, legal and technological updates may need to be incorporated more frequently.

Version	Date	Approved by
1.0	02/02/2021	Nadia Brown – Project Manager