Brainkind

Social Media Policy (Service Users

Ver1.0 August 2016

15.10.2023

Digital Communications Manager

Document type:	PPG Name
Version:	1.0
Primary Sponsor:	Digital Communications Manager
Co-Sponsors:	
Approved by:	Rich Jane
Date Policy Implemented:	August 2016
Policy Review Date:	July 2024 (30 days before expiry date)
Policy Expiry Date:	August 2026
Date uploaded to Portal:	August 2024
Review Frequency:	3-year review

Version	Date	Type of change	Revisions since previous
Ver 1.0	August 2016	Major update	Policy drafted

Contents

2 Introduction

Websites and applications that enable users to create and share content or to participate in social networking are known as social media. Social media platforms such as (but not limited to) Twitter, Facebook, LinkedIn, Pinterest and Instagram offer Brainkind and its staff and service users a range of opportunities.

For service users these platforms offer:

- a channel to stay in touch with friends, family, colleagues or other contacts and with wider news and information (particularly important
- for those who are severely physically disabled with communication problems).
- a chance to celebrate successes and (where appropriate) a means of supporting rehabilitation or reablement
- an opportunity to find out more about the wider work of Brainkind
- the chance to develop or relearn skills or knowledge which may have been lost or impaired.

Brainkind itself uses social media channels to promote the work of Brainkind, including service user case studies and information, to engage with existing audiences and reach new ones in line with agreed marketing plans and wider communications activity. Fuller details are set out in the Social Media Policy for Staff. Ideas from staff or service users for the use of new platforms are welcome and should be sent to the Communications team. Advice and ‘tips for use of social media are also provided in Appendix 1.

3 Policy statement

The welfare and wellbeing of service users and staff, and enhancing and protecting the reputation of Brainkind, are the key principles underlying this policy.

Brainkind seeks to encourage the use of social media for the benefit of the organisation and its beneficiaries as part of the promotion of, and delivery of, its services. There are significant advantages in using these platforms, which have global reach and offer instant access to millions of people including specialist or like-minded groups who share an organisation’s or an individual’s interests.

However, there are risks attached to use of social media for the organisation, its staff and service users, in relation to the safeguarding of children and adults. Therefore, this policy should be operated in conjunction with Brainkind's operational Policies and Procedures, in particular any safeguarding issues related to social media (for example cyber bullying and trolling) should be dealt with using Brainkind's Safeguarding Policies and Procedures. If in doubt, advice about the operation of social media should be sought from Brainkind's Communications team.

4 Scope

This policy applies to:

- All service users within Brainkind's services

5 Definitions

Term	Definition
Platform or channel	Generic term for a social media website or application
Post or share	Upload text, photos, graphics, videos, weblinks or associated or similar information which are immediately published on a social media platform
Permissions	Permissions received from staff or service users to publish material related to them, including images, under the Data Protection Act 1988 and permissions associated with copyright legislation and the publication of material owned by others.
Account	The electronic means by which an individual's (or organisation's) activity on a social media platform is run

Trolling	Posting inflammatory or disruptive comments online with the deliberate intention of upsetting or disturbing others
Material	Text, photos, graphics, videos, weblinks or associated or similar information

6 Responsibilities

Role	Responsibilities and accountabilities
The Chief Executive Officer (CEO) & Executive Leadership Team (ELT)	To ensure that systems and processes are in place to oversee and ensure safe and appropriate use of social media.
All Managers	To ensure that the benefits of social media are considered and its use, where appropriate, is clearly referenced within support/reablement/rehabilitation plan To manage staff use of social media in relation to its impact in the workplace and on others, as outlined within this Policy.
All staff	To assist and support service users to implement their rights to access social media in line with their support/reablement/rehabilitation plan, this Policy and associated good practice. To be aware of the benefits and risks of social media in a professional context and to operate this policy in conjunction with Brainkind's safeguarding policies and procedures To be aware that if misuse is suspected or breach of this policy has occurred, disciplinary action may be taken, in line

	with Brainkind's Disciplinary Policy and Procedure. To report significant issues or good practice concerning the operation of social media via their manager to Brainkind's Digital Communications Manager or Director of Communications.
Service Users	To use social media if they wish and to follow the best practice contained in Appendix 1 and the Social Media policy outlined below
Clinical staff	To consider social media use as part of support/reablement/rehabilitation plans as appropriate and as set out within the policy.

7 Procedure

7.1 Social media use as part of support plans

Continuing or renewing contact with friends and family, learning new skills or knowledge and engaging with people across the country and the globe can be of enormous benefit to service users.

For these reasons, social media use should, where appropriate, be considered as part of each service user's support/reablement/rehabilitation plan.

In relation to the use of social media, consideration should be given to:

- The benefits and risks to both the individual service user and other service users
- The skill and knowledge level of the service user in relation to social media
- The amount of time, and the nature of the platforms to which the service user has access, and on which equipment and connection (for example on his or her own device using restricted Trust Internet Access or own device using own connection with no restrictions)
- The degree of staff supervision and support required in order to enhance service user independence while safeguarding the welfare of the individual and others.

- The skill and knowledge level in relation to social media and internet safety of any staff providing supervision and support.

7.2 6.2 Data protection, permissions, and copyright

If any individual want to post photos or film or similar material online of other people, then their permission must be gained before it is posted. Materials published online including images, photographs and graphics are subject to copyright law and great care should be taken if reproducing, publishing or sharing material where the individual doing so does not own the copyright (for example, uploading music tracks or photos created by someone else). Appropriate checks should be made and permissions sought by the individual posting the material if there is any doubt.

7.3 6.3 Managing risk

It is important to note that Trust service users are vulnerable adults (or in the case of Brainkind's school, children) who are potentially at risk when they access social media, even if they are over the minimum age prescribed by certain channels, due to:

- Cyber bullying (as victims or perpetrators)
- Temptation to visit adult themed websites that feed addictive behaviours, such as online gambling, adult sites or sites promoting illegal activity
- Viewing content that could impede their rehabilitation or reablement progress
- Contacting or being contacted by people who want to exploit their vulnerability
- Not knowing who they are talking to (care should be taken when using messaging apps like WhatsApp or similar, or with any personal messaging which is not public, that the individual knows and trusts the person they are talking to)
- Sharing too much personal information online (care should be taken to ensure the right privacy settings have been made in relation to public facing content)
- Potentially using offensive language or unwittingly sharing images that some may find upsetting
- Sharing material about other service users or staff who may not have given the appropriate permissions or which may otherwise be inappropriate.

Support/reablement/rehabilitation plans should evidence, for cases of people who have depended on social media for wellbeing, that the risks around using social media are managed, given the negative effect social media can have on mood and motivation. Social media needs to be included on the appropriate risk assessment matrix where and when relevant, and this risk assessment will trigger the associated support arrangements which should be contained within the service user's support/reablement/rehabilitation plan and associated records; this should also specify what support and supervision/restrictions might be advisable in light of any service user's specific brain and social problems. The arrangements should be reviewed regularly; it should be borne in mind that social media issues can develop very quickly and daily of more frequent checks may need to be made.

Care should be taken to manage social media contact between service users as this can be a channel for inappropriate behaviour towards others.

The Mental Health Act, Mental Capacity Act and Deprivation of Liberty Safeguards, where relevant, together with associated Trust Policies and Procedures must also be followed when considering access to social media.

Abusive and/or potentially criminal activity should be reported in line with Brainkind's safeguarding policies

Abuse can also be reported online using the 'Report' buttons which appear on most social media channels and staff should support service users to do this as appropriate; other social media users can be 'blocked' if needed and information on how to do this is contained on most social media sites. If in doubt, advice should be sought from the Communications team.

7.4 Setting up local-based social media accounts to safeguard service users

Staff may set up a locally-based social media account in a professional capacity, including set up of a generic (eg Gmail, Hotmail or similar) email account, in order to follow a service user on a social media channel, if:

- this is deemed necessary to safeguard the wellbeing and welfare of the service user to be decided within the Multi-Disciplinary Team (MDT) or equivalent care planning process, which will be clearly recorded in the service user records, and
- this arrangement has the service user's consent.

Any such email account must only be used for purposes connected to the welfare and wellbeing of the service user in relation to social media. Records of these arrangements, including log-in details, must be kept as part of the risk assessment

and support/reablement/rehabilitation plan, and be subject to the appropriate Clinician or Service Manager authorisations, so that the relevant staff have access to the account. It must not be used to post material.

The appropriate Mental Health Act and Mental Capacity Act and the associated Trust Policies and Procedures must also be followed when considering service user consent.

7.5 Misuse or abuse of social media

Service users may use Trust ICT equipment designated for service users and Trust wifi/data connections to access social media only for lawful purposes and may not use our wfi or data connections for the following purposes:

- In any way that breaches any applicable local, national or international law or regulation.
- In any way that is unlawful or fraudulent, or has any unlawful or fraudulent purpose or effect.
- For the purpose of harming or attempting to harm minors in any way.
- To transmit, or procure the sending of, any unsolicited or unauthorised advertising or promotional material or any other form of similar solicitation (spam).
- To knowingly transmit any data, send or upload any material that contains viruses, Trojan horses, worms, time-bombs, keystroke loggers, spyware, adware or any other harmful programs or similar computer code designed to adversely affect the operation of any computer software or hardware.

Service users may also use their own devices and/or his or her own data service (for example 3G/4G or similar) to access social media platforms

However, if access to social media (whichever the equipment or wifi/data connection) is used to post unlawful, inappropriate, offensive or threatening material, Trust staff should intervene in line with the support/reablement/rehabilitation plan in place and in line with Brainkind's safeguarding policies.

In extreme cases, if while on Trust premises a service user repeatedly misuses or abuses social media and/or uses social media to bully or bring distress to others and/or damage the reputation of Brainkind, Brainkind reserves the right to withdraw access to the equipment and/or data/wifi connection (whether owned by Brainkind or not), or to review and where necessary terminate a placement.

7.6 Social media 'friending/following' between service users and staff

In order to maintain appropriate professional conduct, under no circumstances should staff become 'friends/fans/followers' with former or current service users, or former or current service users' family or friends, on social media using their personal social media channels Staff feeling undue pressure to become 'friends/fans/followers' in these circumstances should speak to their line manager.

7.7 Staff use of service user equipment/service user use of staff owned or allocated equipment

Under no circumstances should service user equipment be used by Trust staff to access social media sites for personal use, even if the service user has given permission. Similarly, staff should not allow service users to use equipment owned by staff, or Trust devices specifically allocated to staff, to access social media. The Mobile Phone Usage at Work Policy and Social Media Policy for Staff also applies in these circumstances. If access to such equipment is provided in breach of Trust policies, Brainkind reserves the right to invoke disciplinary proceedings

8 References and associated Policies and Procedures

- Information Technology Policy
- Internet and Email Policy
- Complaints and Compliments Policy and Procedure
- Safeguarding Adults at Risk Policy and Procedure/safeguarding
- Children at Risk Policy and Procedure
- Disciplinary Policy and Procedure
- Mental Health Act Policy
- Bullying and Harassment Policy
- Mobile Phone Usage at Work Policy
- Social Media Policy for Staff
- Heathermount School E-safety Policy

9 Monitoring, audit and review

This policy remains under the control of the Communications team and resides within Brainkind's intranet known as the Hub.

The QA division maintains the document control database for tracking and monitoring Brainkind-wide controlled documents within the Hub.

It is the responsibility of Divisional governance teams to audit compliance with all policies as part of their normal audit cycle and undertake remedial action as required.

10 Equality Impact Assessment Statement

As part of its development, this policy and its impact on equality have been reviewed in line with Brainkind's Equality and Diversity Policy. The purpose of the assessment is to minimise and if possible remove any disproportionate impact on service users and people employed by Brainkind on the grounds of race, sex, disability, age, sexual orientation or religious belief. This policy was reviewed and no detriment was identified.

		Yes/No	Comments
1.	Does the policy/guidance affect one group less or more favourable than another on the basis of:		
	Race	No	
	Ethnic Origns (including gypsies and travellers)	No	
	Nationality	No	
	Gender	No	
	Culture	No	
	Religion or belief	No	
	Sexual orientation including lesbian, gay and bisexual people	No	

	Age	No
	Disability - learning disabilities, physical disability, sensory impairment and mental health problems	No
2.	Is there any evidence that some groups are affected differently?	No
3.	If you have identified potential discrimination, are any exceptions valid, legal and/or justifiable?	N/A
4.	Is the impact of the policy/guidance likely to be negative?	No
5.	If so can the impact be avoided?	N/A
6.	What alternatives are there to achieving the policy/guidance without the impact?	N/A
7.	Can we reduce the impact by taking different action	N/A

11 Revision History

Version	Summary of Changes	Approver	Revision Date

12 Appendix 1

10 Top Tips for using social media safely

1.Think before you post Don’t upload or share anything you wouldn’t want your family or friends seeing. Once you press send or post, you are publishing the information - it is no longer private!

2.Check your settings Use the privacy and security settings on social media sites so that only friends and family can see your pages. Then encourage your friends / family / colleagues to tighten their privacy settings too as they could affect you. Even if your account is locked as private, personal information you have shared with others could still be accessed through their pages.

3.Be careful what you share online When you choose a profile picture for a social networking website like Facebook or Twitter, avoid photos that could give strangers clues about where you live or are staying. Check your privacy settings regularly. Think about what should be shared in public and what shouldn't.

4.Never share or reveal your passwords Use strong passwords that are hard for others to guess, using a mix of letters and numbers. Keep passwords to yourself and change them regularly.

5.Be careful who you chat to If somebody you don’t know adds you as a friend, ignore them and delete their request. Don’t share personal information like your address or phone number with somebody you don't know, and be cautious of people you’ve just met online who want to meet you very quickly.

6.Photos and videos Be careful about which photos and videos you share on social media sites - avoid photos of your home, or places you're associated with. Remember, once you've put a picture of yourself online, other people may be able to see it and download it - it may not just be yours anymore. If other people are in the photo/video, make sure they’re happy for you to share it online before you post it.

7.Check what’s needed Don't give out information online simply because it's asked for - think whether whoever is asking for it, really needs it. When you're filling in forms online, for example to register with a website or sign up for a newsletter, always provide the minimum information possible.

8.Direct message if you can It's almost always possible to send a direct (private) message on social media platforms. If you're having a personal chat, and you know and trust who you are talking to, this is the best option to go for

- unless you don't mind sharing your conversation with millions of other users. Alternatively, send an email from a private account.

9.Delete old accounts Create separate email accounts for each social networking site that you register to use. This way if you want to close down a particular social media profile and stop receiving messages from that account, you can simply stop using that email account. It is easy to set up a new email account through Gmail, Hotmail, or Yahoo! Mail. Once you stop using a social media site or forum,

remember to close your account down. There's no point in leaving personal information out there unnecessarily.

10. Get anti-virus software Make sure you have anti-virus software installed on your computer and be careful what you download or install on your device.

Further information: https://www.getsafeonline.org/ https://www.thinkuknow.co.uk/ (for children but has some useful information) http://www.safernet.org.uk/ (for people with learning disabilities)