



SOCIAL MEDIA POLICY

BADGER GROUP
Badger House
121 Glover Street
Birmingham, B9 4EY

Destroy All Previous Issues

This document is the property of Badger and must not be reproduced, published or used by any third party without prior written authorisation from Badger.

Author	Issue Date	Version	Document Ref	Approved By	Approval Date	Next Review	Page i
IT Department	Oct 2023	V1.1	IT-PO-03	IT Dept/HR	Oct 2023	Oct 2024	

Contents

1	INTRODUCTION / about this policy	1
2	PERSONNEL RESPONSIBLE FOR IMPLEMENTING THE POLICY	1
3	COMPLIANCE WITH RELATED POLICIES AND AGREEMENTS	1
4	PERSONAL USE OF SOCIAL MEDIA	2
5	PROHIBITED USE	2
6	BUSINESS USE OF SOCIAL MEDIA	2
7	GUIDELINES FOR RESPONSIBLE USE OF SOCIAL MEDIA	2
8	MONITORING	3
9	RECRUITMENT	3
10	BREACH OF THIS POLICY	3

DOCUMENT CONTROL

Document Storage

Location: p:\ops team\central policies & procedures - development - word docs\it policies\it-po-03 social media policy v1.1.docx

Version Control Log (Only last 3 versions, earlier versions can be found in the appropriate Archive directory for the document)

Version	Date	Author	Description of Changes
V1.0	July 2022	Doc Control	Original version was previously HR-46 (HR Policies) it was agreed this should come under IT with immediate effect
V1.1	Oct 2023	S Hemming / S Parmar	Reviewed by Head of Technology / Director of Workforce

Approval

Version	Name	Position	Signature	Approved Date

Glossary

Term	Description

1 INTRODUCTION

- 1.1 This policy is in place to minimise the risks to our organisation through use of social media.
- 1.2 This policy deals with the use of all forms of social media, including Facebook, LinkedIn, X (formally known as Twitter), Google+, Wikipedia, Instagram, TikTok and all other social networking sites, internet postings and blogs. It applies to use of social media for business purposes as well as personal use that may affect our organisation in any way.
- 1.3 This policy covers all employees, officers, consultants, contractors, volunteers, apprentices, work experience, casual workers and agency workers.
- 1.4 This policy does not form part of any employee's contract of employment and we may amend it at any time.

2 PERSONNEL RESPONSIBLE FOR IMPLEMENTING THE POLICY

- 2.1 The board of Directors has overall responsibility for the effective operation of this policy, but has delegated day-to-day responsibility for its operation to the Head of Technology.
- 2.2 Responsibility for monitoring and reviewing the operation of this policy and making recommendations for change to minimise risks lies with the Head of Technology who will review this policy annually to ensure that it meets legal requirements and reflects best practice.
- 2.3 Managers have a specific responsibility for operating within the boundaries of this policy, ensuring that everyone understands the standards of behaviour expected of them and acting when behaviour falls below its requirements. Managers will be given training to do this.
- 2.4 Everyone is responsible for the success of this policy and should ensure that they take the time to read and understand it. Any misuse of social media should be reported to the Line Manager immediately after becoming aware. They will seek guidance from HR and or the IT Department. Questions regarding the content or application of this policy should be directed to either HR or the Head of Technology.

3 COMPLIANCE WITH RELATED POLICIES AND AGREEMENTS

- 3.1 Social media should never be used in a way that breaches any of our other policies. If an internet post would breach any of our policies in another forum, it will also breach them in an online forum. For example, you are prohibited from using social media to:
 - breach our IT and Communications Systems Policy;
 - breach our obligations with respect to the rules of relevant regulatory bodies;
 - breach any obligations contained in those policies relating to confidentiality;
 - breach our Disciplinary Policy or procedures;
 - harass or bully other staff in any way;
 - unlawfully discriminate against other staff or third parties;
 - breach our Data Protection Policy (for example, never disclose personal information about a colleague online);or
 - breach any other laws or regulatory requirements.
- 3.2 You should never provide references for other individuals on social or professional networking sites, as such references, positive and negative, can be attributed to the organisation and create legal liability for both the author of the reference and the organisation.

- 3.3 Anyone who breaches any of the above policies will be subject to disciplinary action up to and including termination of employment.

4 PERSONAL USE OF SOCIAL MEDIA

Occasional personal use of social media during working hours using personal equipment only is permitted so long as it does not involve unprofessional or inappropriate content, does not interfere with your employment responsibilities or productivity and complies with this policy.

5 PROHIBITED USE

- 5.1 You must avoid making any social media communications that could damage our organisations interests or reputation, even indirectly.
- 5.2 You must not use social media to defame or disparage us, any member of the organisation or any third party; to harass, bully or unlawfully discriminate against staff or third parties; to make false or misleading statements; or to impersonate colleagues or third parties.
- 5.3 You must not express opinions on our behalf via social media, unless expressly authorised to do so by your manager.
- 5.4 You must not post comments about sensitive organisational-related topics, such as our performance, or do anything to jeopardise our trade secrets, confidential information and intellectual property. You must not include our logos or other trademarks in any social media posting or in your profile on any social media.
- 5.5 Any misuse of social media should be reported to your Line Manager immediately after becoming aware. The Line Manager will then seek guidance from the HR Department and or the IT Department to assist in any investigation.

6 BUSINESS USE OF SOCIAL MEDIA

- 6.1 If you are contacted for comments about the organisation for publication anywhere, including in any social media outlet, direct the enquiry to the Quality and Compliance Team and do not respond without written approval.
- 6.2 The use of social media for organisational purposes is subject to the remainder of this policy.

7 GUIDELINES FOR RESPONSIBLE USE OF SOCIAL MEDIA

- 7.1 You should make it clear in social media postings, or in your personal profile, that you are speaking on your own behalf. Write in the first person and use a personal email address.
- 7.2 Be respectful to others when making any statement on social media and be aware that you are personally responsible for all communications which will be published on the internet for anyone to see.
- 7.3 If you disclose your affiliation with us on your profile or in any social media postings, you must state that your views do not represent those of us. You should also ensure that your profile and any content you post are consistent with the professional image you present to patients and colleagues.
- 7.4 If you are uncertain or concerned about the appropriateness of any statement or posting, refrain from posting it.

- 7.5 If you see social media content that disparages or reflects poorly on us, you should contact your Line Manager immediately on becoming aware.

8 MONITORING

- 8.1 We reserve the right to monitor, intercept and review, without further notice, staff activities using our IT resources and communications systems, including but not limited to social media postings and activities, to ensure that our rules are being complied with and for legitimate business purposes and you consent to such monitoring by your use of such resources and systems.
- 8.2 For further information, please refer to our IT and Communications Systems Policy.

9 RECRUITMENT

We may use internet searches to perform due diligence on candidates in the course of recruitment. Where we do this, we will act in accordance with our data protection and equal opportunities obligations.

10 BREACH OF THIS POLICY

- 10.1 Breach of this policy may result in disciplinary action up to and including dismissal. Any member of staff suspected of committing a breach of this policy will be required to co-operate with our investigation, which may involve handing over relevant passwords and login details.
- 10.2 You may be required to remove any social media content that we consider to constitute a breach of this policy. Failure to comply with such a request may result in disciplinary action.