

# **Benevolent<sup>AI</sup>**

---

## **SOCIAL MEDIA POLICY**

---

## 1. INTRODUCTION

1.1 BenevolentAI (the “**Company**” and, together with its subsidiaries, the “**Group**”, **we**”, “**us**” and “**our**”) has prepared this social media policy (this “**Policy**”) to minimise the risks to its business through the use of social media.

1.2 This Policy deals with the use of all forms of social media, including but not limited to, Facebook, LinkedIn, Twitter, Google+, Wikipedia, YouTube, Instagram, Reddit and all other social networking sites, internet postings, blogs, messaging applications and media sharing sites. It applies to use of social media for business purposes as well as for personal use.

1.3 The Group understands and fully respects the rights of staff of Group companies to engage in social media activity. However, the Group is conscious that members of staff engaging in social media activity could adversely affect its legitimate business interests in certain circumstances. Also, certain readers could mistakenly view a member of staff as a spokesperson of the Group. Owing to the great value that we place on our reputation and goodwill, social media activity is a key focus of Group policy.

1.4 This Policy covers all employees, officers, consultants, contractors, volunteers, interns, casual workers and agency workers.

1.5 This Policy is not contractual and does not form part of any employee's contract of employment. The Group may vary or amend this Policy at its discretion and may apply it as far as practicable in the circumstances.

## 2. PERSONNEL RESPONSIBLE FOR IMPLEMENTING THE POLICY

2.1 The Company's board of directors has overall responsibility for the effective operation of this Policy, but has delegated day-to-day responsibility for its operation to Chief People Officer.

2.2 Responsibility for monitoring and reviewing the operation of this Policy and making recommendations for change to minimise risks lies with the People Director who will review this Policy on at least an annual basis to ensure that it meets legal requirements and reflects best practice.

2.3 Directors have a specific responsibility for operating within the boundaries of this Policy, ensuring that all staff understand the standards of behaviour expected of them and taking action when behaviour falls below its requirements.

2.4 All staff are 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 CLIP team.

### 3. PERSONAL USE OF SOCIAL MEDIA

The Group provides IT equipment and services primarily for business use. Colleagues are permitted some incidental use of the Group's devices such as to send personal emails, browse the internet, or access social media platforms. Personal use is a privilege and not a right. It must not be overused or abused. We may withdraw permission for it at any time or restrict access at our discretion.

3.1 Incidental use may be defined by the following conditions:

- (a) Use must be minimal and take place substantially out of normal working hours (that is, during lunch breaks, before 9 am or after 5.30 pm).
- (b) Personal emails should be labelled "personal" in the subject header.
- (c) Use must not interfere with business or office commitments.
- (d) Use must not commit us to any marginal costs.
- (e) Use must comply with the requirements set out in the inappropriate information section of our IT Acceptable Use Policy.
- (f) Use must not adversely affect the reputation of the organisation.

3.2 Prohibited use:

Social media should never be used in a way that breaches any of the Group's other policies. If an internet post would breach any of the Group's policies in another forum, it will also breach them in an online forum. For example, you are prohibited from using social media to:

- (a) breach the Group's disciplinary policy or procedures;
- (b) breach the Group's IT Acceptable Use Policy;
- (c) breach the Group's obligations with respect to the rules of relevant regulatory bodies;
- (d) breach any obligations contained in those policies relating to confidentiality;
- (e) harass or bully other colleagues in any way;
- (f) breach the Group's Equality, Diversity and Inclusion Policy / unlawfully discriminate against other staff or third parties;
- (g) breach the Group's Data Protection Policy (for example, never disclose personal information about a colleague online); or
- (h) breach any other laws or regulatory requirements.

3.3 You must avoid making any social media communications that could damage the Group's business interests or reputation, even indirectly.

3.4 You must not use social media to defame or disparage us, the Group's staff 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.

3.5 You must not express opinions on the Group's behalf via social media, unless expressly authorised to do so by your manager or anyone with the authority to grant such authorisation. You may be required to undergo training in order to obtain such authorisation.

3.6 You must not post comments about sensitive business-related topics, such as the Group's performance, or do anything to jeopardise the Group's trade secrets, confidential information and intellectual property or which could give a competitive advantage to other companies (e.g. financial information, strategies and business plans, legal issues and future plans). You must not include the Group's logos or other trademarks in any social media posting or in your profile on any social media.

3.7 You must not post confidential or non-public information (for example, this may include part of the Group's code or anything closely related to the Group's code, or any information related to specific drug targets or programmes that the Group is working on or interested in). As a general rule, if it is not on the Group's website, do not post it.

3.8 Any misuse of social media should be reported to the People team via your People Partner.

#### **4. PERMITTED USE**

4.1 Our Messaging Guidelines contains a full overview of what can be publicly disclosed about the Group.

4.2 Examples of what can be publicly disclosed about the Group include:

- (a) Sharing any posts appearing on the BenevolentAI social channels.
- (b) Posting links to the BenevolentAI website. This also applies to job vacancies, as the Group has a referral scheme and your network could be interested in jobs at the Group.
- (c) Posts about life at BenevolentAI (e.g. posts that focus on office drinks, Lunch & Learns, internal campaigns such as IWD/Pride/Black History Month). Whilst taking pictures in the office is permissible, please refrain from posting any pictures of whiteboards, screens or which otherwise reveal confidential information. Please ask your colleagues for permission before posting any pictures of them on social media.

- (d) Posts about key moments or milestones, provided it is already in the public domain (e.g. progress in the Group's collaborations, published research papers, information disclosed on the Group's pipeline page and case studies).
- (e) Sharing or posting about events where you or your colleagues are attending or speaking.

4.3 We encourage blogging on behalf of BenevolentAI on the Group's corporate channels (such as the Group's website or Medium page), and permit blogging on your personal channels, but please note the following requirements:

(a) **Blogging on BenevolentAI's own channels**

(i) Our corporate channels target specific audiences and blogging will generally centre around topics such as:

- (A) Thought leadership in AI-drug discovery and related fields
  - (B) Life and culture at BenevolentAI
  - (C) Data diversity
  - (D) Domain-specific technology or science topics (e.g. the Group's engineering blog)
- (ii) These topics are curated by the Group's Communications team who will assist you with navigating the process. The blog will also require approval by the communications and CLIP team prior to being posted.
- (iii) If you would like to suggest a blog please, contact [communications@benevolent.ai](mailto:communications@benevolent.ai)

(b) **Blogging on external outlets on behalf of, or about, BenevolentAI**

If you receive an invitation to write a blog on behalf of, or about, BenevolentAI, please contact the Communications team before accepting the invitation. The Communications team will need to authorise your involvement, and approve the content before the blog is shared with the external outlet.

(c) **Blogging on your personal channels about BenevolentAI**

If you would like to blog about the company's work or about your individual job/skill sets used at BenevolentAI on your own channels, you are free to do so, provided that: (i) the blog adheres to the requirements of this Policy (especially in relation to what can and cannot be disclosed); and (ii) you have received approval from the CLIP and communications team before publishing the blog.

(d)  **Blogging on your personal channels about other topics**

You are free to blog any other topic, provided that the blog adheres to the requirements of this Policy.

4.4 The use of social media for business purposes is permitted in accordance with paragraph 6 below.

**5. BUSINESS USE OF SOCIAL MEDIA**

5.1 If your duties require you to speak on behalf of us in a social media environment, you must still seek approval from the Communications team, who may require you to undergo training before you receive approval and impose certain requirements and restrictions with regard to your activities.

5.2 Likewise, if you are contacted for comments about the organisation for publication anywhere, including in a social media outlet, direct the enquiry to the Communications team and do not respond without written approval.

5.3 The use of social media for business purposes is subject to the remainder of this Policy.

**6. GUIDELINES FOR RESPONSIBLE USE OF SOCIAL MEDIA**

6.1 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.

6.2 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.

6.3 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 your employer (unless you are authorised to speak on behalf of the Group as set out in paragraph 4.4 above). Typically, in your social profile you can add a statement such as: “Views are my own”. You should also ensure that your profile and any content you post are consistent with the professional image you present to clients and colleagues.

6.4 Please keep in mind:

(a) There’s no such thing as a “delete” button on the internet, so please—always pause and think before posting.

(b) Some subjects can invite inflammatory responses. When discussing topics where emotions run high (e.g., politics and religion), remember to show respect for others’ opinions.

(c) Remember that the internet is global, and what you say can be seen by people all over the world. Something you say in one country might be inaccurate or offensive in another.

6.5 If you are uncertain or concerned about the appropriateness of any statement or posting, refrain from posting it until you have discussed it with your manager or a member of the Communications team.

6.6 If you see social media content that disparages or reflects poorly on us; do not answer directly. Instead, you should contact [communications@benevolent.ai](mailto:communications@benevolent.ai). We will help assess whether or not we should respond.

## **7. MONITORING**

We reserve the right to monitor, intercept and review, without further notice, staff activities using the Group's IT resources and communications systems, including but not limited to social media postings and activities, for legitimate business purposes which include ascertaining and demonstrating that expected standards are being met by those using the systems and for the detection and investigation of unauthorised use of the systems (including where this is necessary to prevent or detect crime). See our IT Acceptable Use Policy for further details.

## **8. RECRUITMENT**

The Group may use internet searches to perform due diligence on candidates in the course of recruitment. Where this is done, the Group will act in accordance with its data protection and equal opportunities obligations.

## **9. BREACH OF THIS POLICY**

9.1 Breach of this Policy may result in disciplinary action, up to and including termination of employment.

9.2 You may be required to remove any social media content that the Group considers to constitute a breach of this Policy. Failure to comply with such a request may result in disciplinary action.

## **10. QUESTIONS**

In case of any questions in relation to this Policy, please contact the Communications Team.

**Approved by the Board on 12 March 2024.**