SOCIAL MEDIA POLICY

1. About this policy

1.1 The purpose of this policy is to minimise the risks to The Mainstay Foundation (the Charity) through use of social media. This policy applies to the use of all forms of social media, including all social networking sites, internet postings and blogs. It applies to the use of social media for the Charity's purposes as well as personal use that may or potentially affect the Charity in any way.

1.2 This policy does not form part of any contract of employment or other contract to provide services, and we may amend it at any time.

2. Who does this policy apply to?

2.1 This policy applies to all employees, officers, consultants, self-employed contractors, casual workers, agency workers, volunteers and interns.

3. Who is responsible for this policy?

3.1 The Board of Trustees has overall responsibility for the effective operation of this policy. The Board has delegated responsibility for overseeing its implementation to the Executive Officer. Questions about the content of this policy or suggestions for change should be reported to the Executive Officer.

3.2 You should refer any questions you may have about the day-to-day application of this policy (including reporting the misuse of social media) to your immediate line manager in the first instance.

4. Compliance with related policies and agreements

4.1 You should never use social media in a way that breaches any of our other policies. If an internet post would breach any of our policies in another forum, it would also breach them in an online forum. For example, you are prohibited from using social media to (the following is not an exhaustive list):

(a) breach any obligations we may have with respect to the rules of relevant regulatory bodies;

(b) breach any obligations contained in those policies relating to confidentiality;

(c) breach our disciplinary procedures;

(d) harass, intimidate or bully other staff or third parties in any way;

(e) unlawfully discriminate against other staff or third parties;

(f) breach our Data Protection Policy (for example, you should never disclose personal information about a colleague or others online);

(g) post offensive, libellous or defamatory comments (or which have the potential to be construed as such);

(h) breach copyright, so you should never post material that is owned by another person or organisation without written permission; or

(i) breach any other laws or regulatory requirements.

4.2 You should never provide references for other individuals on social or professional networking sites. These references, positive and negative, can be attributed to the Charity and create legal liability for both the author of the reference and the Charity.

5. Personal use of social media

Occasional personal use of social media during working hours 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.

6. Prohibited use

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

6.2 You must not use social media to:

(a) defame or disparage the Charity, our staff or any third party;

(b) harass, bully or unlawfully discriminate against staff or third parties;

(c) make false or misleading statements; or

(d) impersonate colleagues or third parties.

6.3 You must not express opinions on our behalf via social media, unless expressly authorised to do so by the Executive Officer and Executive Trustee. You may be required to undergo training to obtain this authorisation.

6.4 You must not post comments about sensitive related topics in relation to the Charity or its operations, such as our performance, or do anything to jeopardise our confidential information including but not limited to our donors, partners and beneficiaries. You must not include our logos or other trademarks in any social media posting or in your profile on any social media.

6.5 The contact details of business contacts made during the course of your employment are our confidential information. On termination of employment, you must provide us with a copy of all that information, delete all that information from your personal social networking accounts and destroy any further copies of that information that you may have.

7. The Charity's use of social media

7.1 All social media activity must adhere to the General Data Protection Regulations (GDPR), the Privacy and Electronic Communication Regulations (PECR), the Fundraising Regulator, the Equality Act 2010, as well as copyright and defamation laws. Additionally, it must comply with the Charity's internal policies and the rules of social media platforms. Only trained and authorised individuals may upload content, and all posts in addition to any written element such as captions, image text, or voiceovers in multimedia must undergo internal review and authorisation by both the Executive Officer and Executive Trustee before publication.

7.2 As a faith organisation, the Charity should only post social media content in line with the objects. All content must reflect these principles and must not be perceived as violating them. Any content breaching these principles will be removed. Any posts which are or can be construed to be political in nature should be avoided. Sensitive topics, particularly conflicts, must be addressed with care, and all language used in such contexts requires prior written approval.

7.3 No images that could cause harm or distress, such as those depicting extreme suffering, injuries, nudity, or abuse, may be published or shared. Images of individuals receiving services from the Charity may only be used with their written consent, and their real names or exact locations should be withheld whenever possible to safeguard their identities. Images of children should only be posted with extreme care and only with the parent/guardian's written consent.

7.4 Third-party content of any kind may only be shared after conducting due diligence on both the account holder and the content being shared. As with all social media posts, the approval from both the Executive Officer and Executive Trustee is required prior to sharing. A review of the account from which the content originates must also be performed to ensure that its content, aims, and objectives do not violate the Charity's guidelines or conflict with its values.

7.5 The Charity's official social media accounts may only follow accounts authorised by the Executive Officer and Executive Trustee. Personal accounts of staff, contractors, volunteers, supporters, or media personalities should not be followed to reduce the risk of reputational damage by association.

7.6 The use of endorsement features, such as the "like" functions, across any platform is strictly prohibited to avoid reputational risks by association.

7.7 Administrators of social media accounts must not share passwords or any other credentials with anyone unless explicitly authorised by the Executive Officer, Executive Trustee or any other member of the Board of Trustees. Care should be taken not to enter passwords in the view of others, particularly in public spaces. Charity issued devices should be used when logging into the Charity's accounts. If personal devices are necessary for access, prior approval must be obtained from Management or a member of the Board of Trustees. Administrators should only log into Charity accounts when performing their contractual duties and must log out immediately afterward. For security reasons, passwords must not be saved on personal devices or set for automatic sign-in.

7.8 If a password is unintentionally or intentionally shared, staff must immediately notify the Executive Officer or Executive Trustee so that the password(s) can be changed to mitigate potential risks. The Board of Trustees should then be informed of the breach, and appropriate actions will be taken based on the situation.

7.9 Administrators may be required to change account passwords at any time and must immediately inform other password holders of the change through secure, encrypted methods. All passwords for official accounts must be stored in a password-protected document accessible only to authorised password holders as well as the Executive Officer and Executive Trustee.

7.10 In the event of hacking, the platform and the Board of Trustees must be notified immediately, and all efforts should be made to regain control of the account. The password should be changed, and a review of the incident should be conducted to identify any security weaknesses and prevent future breaches. Depending on the severity of the incident, a Serious Incident Report (SIR) may need to be submitted to the Charity Commission and/or the Information Commissioner's Office (ICO).

7.11 If your duties require you to speak of or post on behalf of the Charity in a social media environment, you must still seek approval for that communication from the Executive Officer and the Executive Trustee. You may be required to undergo training before you do so and impose certain requirements and restrictions with regard to your activities.

7.12 Likewise, if you are contacted for comments about the Charity for publication anywhere, including in any social media outlet, direct the enquiry to the Executive Officer and do not respond without written approval.

7.13 No individual, including members of the Board of Trustees, may benefit personally from the Charity or its resources, including its social media platforms. This includes using Charity accounts to promote personal accounts or to advance personal, professional, or

business interests, in accordance with Charity Commission guidance and the Charity's Conflict of Interest Policy.

7.14 The Charity takes all necessary steps to protect its reputation, as outlined by Charity Commission guidelines, which recognise reputation as an asset to be managed by the Board of Trustees. Any content that causes reputational damage will be promptly removed, followed by a formal investigation and the implementation of a mitigation plan. In some extreme cases, this may result in the submission of a Serious Incident Report (SIR) to the Charity Commission.

8. Guidelines for responsible use of social media

8.1 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.

8.2 Be respectful to others when making any statement on social media and be aware that you are personally responsible for all communications which are published on the internet for anyone to see.

8.3 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 our behalf as set out in paragraph 6.3). You should also ensure that your profile and any content you post are consistent with the professional image you present to all.

8.4 If you are uncertain or concerned about the appropriateness of any statement or posting, refrain from posting it until you have discussed it with the Executive Trustee.

8.5 If you see social media content that disparages or reflects poorly on us, you should contact the Executive Officer.

9. Monitoring

9.1 We reserve the right to monitor, intercept and review, without further notice, your activities using our IT resources and communications systems, including but not limited to social media postings and activities, for legitimate business purposes which include:

(a) ascertaining and demonstrating that in using the systems you are meeting expected standards; and

(b) the detection and investigation of unauthorised use of the systems (including where this is necessary to prevent or detect crime).

10. 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.

11. Breach of this policy

11.1 Breach of this policy may result in disciplinary action up to and including dismissal. If we suspect you have committed a breach of this policy, you are required to co-operate with our investigation.

11.2 You may be required to remove any social media content that we consider to constitute a breach of this policy. Failure to comply with that request may in itself result in disciplinary action.