Social Media Policy

Document Owner: Grace Foundation
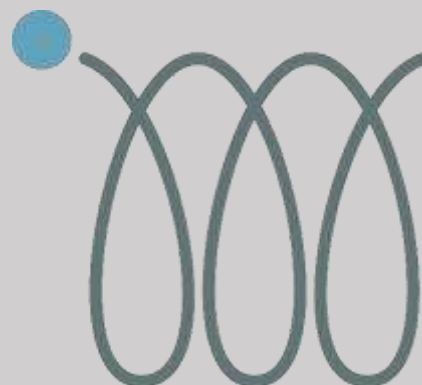
Approved by: Grace Foundation
Board of Trustees

Date Approved: 31/03/2025

Next Review Date: 31/03/2027

Version: 1

Security Classification: Internal use only.

Contents

1. Introduction

This policy outlines Grace Foundation's approach to social media use, ensuring that all online activity aligns with our mission, values, and reputation. It provides guidance to staff, volunteers, and representatives on appropriate and responsible use of social media to support our charitable objectives.

2. Purpose and Scope

Grace Foundation recognises the importance of social media as a tool for communication, engagement, and raising awareness of our work. We are committed to using social media responsibly and professionally while protecting the organisation, its beneficiaries, and its reputation.

This policy seeks to:

- Promote the safe and effective use of social media.
- Safeguard the privacy and dignity of beneficiaries, staff, and stakeholders.
- Prevent misuse of social media that could harm the organisation or its reputation.

This policy applies to:

- All staff, volunteers, and trustees who use social media on behalf of Grace Foundation.
- Both organisational and personal social media accounts when representing or referencing Grace Foundation.

Social Media Platforms Include (but are not limited to): Facebook, Instagram, (X), LinkedIn, TikTok, YouTube, and blogs. It is also includes the use of Artificial Intelligence in relation to social media.

Grace Foundation receives HR, IT, and Financial services from IMG (UK) Holdings Ltd and its subsidiary entities (collectively referred to as IMG). Any mention of IMG in relation to Grace Foundation pertains to these entities.

This policy is entirely non-contractual and does not form part of an employee's contract of employment.

3. Principles for Social Media Use

3.1 Representation of Grace Foundation

- Social media activity should reflect the charity's mission, values, and professional standards.
- Only authorised individuals may post on Grace Foundation's official accounts.

3.2 Respect and Privacy

- Always respect the dignity, privacy, and confidentiality of beneficiaries, staff, and stakeholders.
- Consent must be obtained before sharing images or personal stories of individuals.

3.3 Safeguarding

- Avoid sharing information or images that could put any beneficiary, particularly young people, at risk.
- Staff and volunteers must comply with the organisation's **Safeguarding Policy** when engaging online.

3.4 Transparency and Honesty

- Ensure that all posts are truthful, accurate, and align with Grace Foundation's ethical standards.
- Clearly indicate when posts are sponsored or involve partnerships.

3.5 Appropriate Content:

- Avoid posting content that could be considered offensive, discriminatory, or damaging to the organisation's reputation.
- Political neutrality must be maintained, in line with charity law.

4. Procedures for Social Media Use

4.1 Posting on Official Accounts

- Authorisation: only designated staff (e.g., Executive Assistant) may post on Grace Foundation's official social media platforms.
- Approval: content relating to sensitive topics or major campaigns must be approved by senior management.
- Tone and Style: posts should be professional, inclusive, and consistent with the charity's branding.

4.2 Personal Use of Social Media

Staff and volunteers may mention their connection to Grace Foundation in personal accounts but must:

- Make it clear that views are their own and not those of the charity.
- Avoid sharing confidential information or discussing sensitive topics related to the charity.
- Refrain from engaging in arguments or controversial discussions in relation to Grace Foundation or it's work that could reflect poorly on the charity.

4.3 Managing Risks

- Monitoring: social media accounts will be monitored regularly to ensure compliance with this policy.
- Responding to negative comments:
  - Handle complaints or negative comments professionally and promptly.
  - Escalate serious concerns to the Communications Manager or senior leadership.
- Data Security: use strong passwords for all accounts and ensure access is limited to authorised personnel.

4.4 Use of Images and Stories

- Obtain consent before using all photos or stories of individuals.
- Avoid 'tagging' or identifying minors in posts at all times.

4.5   Crisis Management

In the event of a social media crisis (e.g., offensive posts, hacking, or negative publicity):

- Notify the Communications manager immediately.
- Follow the Serious Incident Reporting Policy if required.
- Issue an appropriate response approved by senior management.

4.6   Training and Awareness

- All staff and volunteers using social media on behalf of Grace Foundation will receive training on this policy.
- Regular updates will be provided to reflect changes in social media trends or legal requirements.

4.7   Compliance and Disciplinary Action

- Any misuse of social media, whether intentional or accidental, that breaches this policy will be addressed through disciplinary procedures.
- Non-compliance may result in restricted access to social media accounts, formal warnings, or other appropriate actions.

4.8   Monitoring and Reporting

- Social media metrics (e.g., engagement, reach) will be reviewed regularly to assess the effectiveness of campaigns.
- Incidents of misuse or risks will be logged and reviewed to improve practices.

5. Use of AI

The following principles should be used to guide the acceptable use of AI:

- Transparency: employees should be transparent about their use of AI. They should disclose to their colleagues and line managers when they are using AI, and they should explain how the AI is being used & ensure that its input and output aligns to GF values.
- Fairness: AI should be used in a fair and non-discriminatory way. Employees should not use AI to make decisions that would unfairly disadvantage certain groups of people.
- Privacy: employees should respect the privacy of individuals when using AI. They should not use AI to collect or store personal data without the consent of the individual.
- Accountability: employees will be accountable for their use of AI. They should be able to explain their decisions and actions, and they will be held responsible for any harm that is caused by their use of AI.

6. Review

This policy will be reviewed every **two years** or sooner if required by changes in social media platforms, regulations, or charity operations.

This policy links to the IMG Safeguarding Policy which can be accessed here.
This policy links to the IMG IT policies (including AI Policy) which can be accessed here.
This policy links to the IMG GDPR policies which can be accessed here.

Approval Date: March 2025
Next Review Date: March 2027