# Global social media policy

December 2021

Sightsavers

# Global social media policy

## Document control

| | |
|---|---|
| **Document owner** | Management |
| **Document administrator** | Director of Campaigning and communications |
| **Document status** | Final |
| **Last reviewed** | November 2021 |
| **Review period** | 1 Year |
| **This version number** | 1.2 |

## Document amendment history

| Version number | Date | Amendment summary | Approved by |
|---|---|---|---|
| 1.0 | 5 December 2018 | Final policy approved | Management Group |
| 1.1 | 26 November 2020 | Final policy amended and approved | Director of Campaigning and communications |
| 1.2 | 1 December 2021 | Final policy amended and approved | Director of Campaigning and communications |

# About this policy

## Introduction

Sightsavers uses social media to raise brand awareness, reach new supporters, steward existing donors and attract new employees. We recognise that those who are involved with Sightsavers' work may also use social media, either as part of their role or in their personal lives, and can be great ambassadors for Sightsavers' work online. That's why we encourage safe, transparent and responsible use of social media to share the organisation's message.

## Why have a social media policy?

Our social media policy is here to encourage the safe and responsible use of social media among anyone connected to Sightsavers who is talking about us online. It's important to remember that we're all ambassadors for the organisation and that social media is a form of public communication.

**This policy aims to help you by:**

- Providing clear guidance on how to talk about the organisation online.
- Complying with relevant legislation in order to protect you.
- Helping you and your line manager understand the potential reputational risks to Sightsavers from social media use.
- Helping you understand where the boundary lies between personal and professional social media use.
- Protecting Sightsavers against liability for the actions of staff.
- Being clear about sensitive issues, such as following staff and volunteer social media accounts.
- Providing guidance on how instances of inappropriate use of social media will be addressed.

## Policy statement

Sightsavers recognises that the internet provides unique opportunities to participate in interactive discussions and share information on particular topics relevant to our work. This activity may involve a wide range of social media such as Facebook, Twitter, Instagram, LinkedIn, YouTube, Tik Tok, blogs, wikis etc. This policy aims to protect individuals working for us in any role, and to encourage you to take responsibility for what you write and exercise good judgement with what you post.

Inappropriate use of social media can pose risks to our confidential and proprietary information and reputation, and can jeopardise our compliance with legal obligations. To minimise these risks, to avoid loss of work time and to ensure that our IT resources and

communications systems are used only for appropriate business purposes, you need to adhere to this policy.

## Other policies

**This policy should be read in conjunction with other Sightsavers policies, including:**

- IT usage policy
- IT security policy
- Information security policy
- Crisis management policy
- Safeguarding policy
- Global discrimination, bullying and harassment policy
- Fundraising policy
- Ethical content policy.

Social media usage needs to be in accordance with these policies.

# Ownership and responsibilities

## Policy owner

Natasha Kennedy, director of campaigning and communications.

## Responsibilities

All staff, trustees, contract workers, work experience staff, volunteers and agencies have a specific responsibility for operating within the boundaries of this policy. We are all responsible for the success of this policy and you should ensure that you take the time to read and understand it.

**Before posting from any Sightsavers social media accounts you must:**

- Have read and understood this policy and other policies listed above.
- Have sought and gained prior approval to do so from the social media manager.
- Completed our social media security GOMO training module.

Any misuse of social media or questions regarding the content or application of this policy should be reported to a line manager, who should also inform the social media manager.

Any content which raises a safeguarding concern must be reported to the safeguarding manager in line with the reporting procedures outlined in Sightsavers' safeguarding policy.

# Scope

This policy covers all staff, volunteers, consultants, contractors and trustees. It covers the use of all forms of social media, including Facebook, YouTube, Twitter, Instagram, LinkedIn, WhatsApp. Tik Tok and all other social networking sites and internet postings, including blogs. It applies to the use of social media both for work and personal purposes, whether while at work or otherwise. The policy applies regardless of whether the social media is accessed using our IT facilities and equipment or equipment belonging to staff.

# Guidelines for use of social media

The following sections of the policy provide you with common-sense guidelines and recommendations for using social media safely and responsibly. A quick guide to talking about Sightsavers on social media is also available on iVillage.

## Content and tone

It's important to remember that social media is a form of public communication – the internet never forgets!

**In particular, you must not post any defamatory statements or posts which are disparaging about:**

- Sightsavers
- Sightsavers' staff (past or present), supporters, beneficiaries, trustees
- Suppliers and vendors
- Other affiliates and stakeholders.

You should also be careful not to post statements which might be misconstrued in a way that could damage Sightsavers' reputation, even indirectly. For instance, statements which do not mention Sightsavers but which are sent from an account which mentions your link to the organisation.

Remember that you must respect confidentiality at all times. Confidential information includes things such as unpublished details about our work, details of current projects, future projects, financial information or information held on our supporters, staff or beneficiaries. Always make sure you've obtained a publicity consent form before sharing images or text about individuals, such as beneficiaries, in posts related to Sightsavers' work on social media.

You are personally responsible for what you communicate on social media (as part of your role or on personal sites). Remember that what you publish might be available to be read by the public (including Sightsavers' supporters and donors), colleagues, future employers, potential employees and social acquaintances for a long time. Keep this in mind before you post content and be mindful about the way that comments about sensitive topics, such as our performance, could be viewed.

If you are uncertain or concerned about a post, wait to share it until you've discussed it with your line manager or the social media manager. It's good practice to avoid publishing anything in the 'heat of the moment' and to revisit posts after a period of time has passed before publishing.

## Accounts and email addresses

There is no obligation for staff to link their personal social media to any Sightsavers social media.

You must speak to the social media manager before setting up social media accounts for work purposes and, if permitted, follow the security procedures outlined in Sightsavers' social media security GOMO module – including setting up two-factor authentication on the account.

If you disclose your affiliation as an employee of Sightsavers on your personal social media account, you should also state that your views do not represent those of the organisation, either within the post itself or as information provided in your social media bio. Remember that by identifying yourself as linked to Sightsavers on social media, you're acting as an ambassador for us online. Also remember that people can still identify you as being connected to Sightsavers even if you don't specifically say you are. For instance, if you are on Twitter but don't mention you work for Sightsavers, but you are also on LinkedIn, where you do, you can't assume the link won't be made.

You are responsible for the security settings of any social media sites you use and should ensure they are set to the appropriate level if you wish to limit who can see your information. You must ensure that all Sightsavers' social media accounts use a strong password, in line with Sightsavers' IT usage and IT security policies. For more information, complete Sightsavers' social media security GOMO training module.

# Reputation management

We are all responsible for protecting Sightsavers' reputation online. If you see content in social media that reflects poorly on Sightsavers or our stakeholders, you should report it to your line manager and/or the social media manager.

If a member of staff is found to be in breach of this policy, their manager may choose to address this using the Global Disciplinary Policy and should seek advice from their HR business partner.

You may be required to remove internet postings which are deemed to constitute a breach of this policy. Sightsavers also reserves the right to request that staff remove reference to Sightsavers on their social media profiles at any time.

# Policy review and update

The social media strategist has overall responsibility for the review and update of this policy at the beginning of each year or more regularly as required.

We work with partners in low and middle income countries to eliminate avoidable blindness and promote equal opportunities for people with disabilities.

www.sightsavers.org

www.sightsavers.org

Registered charity numbers 207544 and SC038110

Sightsavers