

BAS Social Media Policy

Latest update: February 2025

This policy applies to all employees of BAS who use social media. It covers all kinds of use, work-related and personal, where there is potential impact on BAS.

What is social media?

For the purposes of this policy, social media is defined as **any interactive online media** that allows parties to communicate with each other or to share data in a public forum. This includes online social forums, blogs, video and image sharing websites and similar facilities.

Social media is now deeply integrated into everyday life – and it offers many benefits and opportunities for organisations and individuals. It is an **instantaneous**, **permanent**, and **far-reaching** form of communication.

Purpose of this policy

We have a collaborative and encouraging approach to staff **using social media responsibly** - particularly to share information about your role and experiences at British Antarctic Survey.

However, as an employee of BAS, you must be aware that using social media inappropriately could impact upon you, colleagues, and the reputation of BAS.

This policy is intended to:

1. Protect employees and BAS

- 2. Minimise the risk of social media activity which impacts negatively on our reputation
- 3. Help you collaborate with the BAS Communications team, whose job it is to manage BAS reputation

We want you to benefit from social media, while staying within BAS policy. This policy is aligned to the UKRI-NERC and Government Communications Service guidance on the use of social media. Colleagues should be aware of the UKRI policy on personal use of social media.



BAS on social media

The BAS Communications Team use social media as an essential tool for telling the story of British Antarctic Survey to the public and stakeholders.

You can find BAS on the following platforms:

Instagram: @britishantarcticsurvey

LinkedIn: British Antarctic Survey

Facebook: British Antarctic Survey

• Bluesky: @bas.ac.uk

• Threads: @britishantarcticsurvey

YouTube: British Antarctic Survey

Twitter: @BAS_News*TikTok: @we_do_polar*

Digital storytelling is one of the biggest cross-organisational collaborations at BAS, and the Communications team want to work with you to promote and celebrate your work on social media.

You can find the latest information and tips about getting the most out of <u>social media</u> on the IceFlow here.

Your responsibilities

Before posting, ask yourself the following questions:

- 1. Does it have any relation to my work at British Antarctic Survey? And if so, should I tag BAS into my posts?
- 2. Is it clear that I am speaking in my own personal capacity and not on behalf of British Antarctic Survey?
- 3. Could it be contrary to BAS' values?
- 4. Would I be happy to share this with my line manager or colleagues in person?
- 5. Could sharing this have negative consequences for myself or BAS in the future?

^{*} Whilst we have accounts for these channels, BAS is relatively inactive. We keep the accounts for monitoring and to prevent others using our handles to impersonate BAS.



Key guidance for responsible social media use

- 1. Don't post confidential or sensitive information about BAS, including:
 - unpublished scientific research
 - o news stories ahead of an embargo or planned communications activities
 - o medical incidents or evacuations
 - content containing sensitive information, including confidential screen shots, operational information in the background, etc.
 - Zoom meetings without security controls and recordings
 - o commercially sensitive information
- 2. Don't post content in breach of other BAS policies, including:
 - o Images of people without their explicit permission
 - o images of people in our care not wearing appropriate safety equipment*
 - o activities that could be interpreted as being insensitive or discriminatory
 - o activities that could be interpreted as being environmentally damaging
 - images of people working with animals that could be mis-interpreted as unethical
- 3. **State that you work for BAS** if you are posting about the organisation or its work. As well as stating in your profile, you can tag or link to the BAS channels.
- 4. Be clear that the information you post **represents your own views** (e.g. in your bio), and not a corporate BAS view particularly if posting on sensitive or political topics.
- 5. Be clear that you are **not an authorised BAS spokesperson**, unless we ask you.
- 6. **Do not accept media enquiries** without first contacting the Communications Team on press@bas.ac.uk
- 7. Do not accept PR or product endorsements, or pursue monetisation opportunities, without talking to the Communications Team first on communications@bas.ac.uk
- 8. During a major incident, it is essential that you do not independently comment, except to direct to the BAS accounts. The BAS website and social media channels will be the primary source of information, and their use is part of major incident planning. In these circumstances, media, family and staff need a single source of truth.
- 9. Your personal social media can be used for social engineering and phishing. Social networks can also be used to distribute spam and malware. Here's the UKRI guidance.



- 10. You should always comply with UKRI-NERC and BAS policies, including BAS IT Policies, as well as national and international legislation.
- 11. BAS may request that colleagues remove any social media posts, including historic posts, which do not meet these standards.
- 12. We do not tolerate derogatory, discriminatory, bullying, threatening, defamatory, offensive, intimidating or harassing behaviours at BAS online or otherwise.
- 13. BAS' response to any misuse of social media in a personal capacity will be reasonable and proportionate. If unresolved, issues will be escalated to the appropriate director and addressed as a breach of the BAS Code of Conduct and/or breach of contract and may result in further disciplinary action.



Dealing with online 'trolls'

A 'troll' is someone who **deliberately posts provocative, inflammatory, or offensive comments** with the aim of upsetting others, disrupting conversations, or inciting reactions.

Trolls often engage in personal attacks, spread false information, and create conflict within online communities. Their behaviour is typically not aimed at contributing constructively to discussions. You can be the judge of when seemingly 'good faith' questions transition into trolling.

Trolls exploit the natural human instinct of self-defence to provoke response.

To engage and debate does not work, because their goal is for their argument to be heard by as many people as possible. Some platforms, like X, even allow posters to monetise high-engagement posts – leading to a phenomenon known as 'rage-baiting'.

"To directly engage with trolls is to hand them a megaphone. The world would be a happier and less hateful place if, instead of giving these voices the attention and audience they crave, we all simply blocked and ignored them," said Eddie Izzard, comedian, actor, writer and activist.

1. Don't feed the trolls

Engaging amplifies hate. Trolls want attention and followers, not conversation. Reacting or posting about abuse shows trolls that it is working and encourages them to continue.

2. Document and get help if you need

Posts can be deleted, and you may wish to keep a record of the interaction. This will help you get support from HR and Information Security if needed.

3. Block, report, hide and restrict

Each platform gives you different tools to manage this kind of post, so use them freely.

4. Don't let it get to you

It's easy for the online world to feel overwhelming – but conversation there very rarely transfers to offline life. Step away from your devices for a while.



How to spot deepfake media

A **deepfake** is media created using artificial intelligence (AI) to manipulate or create visual and audio content that appears to be real. This can often look like altering videos or images to make it seem like someone is saying or doing something they haven't.

Could it be a deepfake?

- Look for unnatural facial expressions, lip-sync issues, and inconsistent lighting.
- Background: look at lines of perspective, furniture with too many legs, etc.
- Audio that doesn't quite match, usual voice or tone, or odd background noise.
- If you see shocking or out of character content, try to verify it is real before accepting it.

Take measures to protect yourself

- Use multi-factor authentication make it as hard as possible to access your account. Consider an authenticator app.
- Make a conscious, risk-aware decision about your privacy settings and what you post. Any public photo and video content of you builds potential resources for deepfakes.
- Stay up to date with the capabilities of AI generated video to build your awareness.



Social media and the law

Social media is real life – and many protective legal frameworks also apply to behaviour online:

- **Harassment**: Under the Protection from Harassment Act 1997, it is an offence to pursue a course of conduct that amounts to harassment of another person.
- **Malicious communications**: The Malicious Communications Act 1988 makes it an offence to send communications with the intent to cause distress or anxiety.
- **Stalking**: The Protection from Harassment Act 1997 also covers stalking, which involves repeated and unwanted attention that causes distress or fear.
- The Communications Act 2003 makes it an offence to send grossly offensive, indecent, obscene, or menacing messages.

Each social media platform has a variety of tools that allow you to block, report or otherwise limit your contact with those harassing you online.

If you are the victim of persistent poor behaviour online from an individual, the following legal avenues are available to you via reporting to the police – but documentation through screenshots and a dated log will be essential:

- Victims can apply for an injunction to prevent the harasser from continuing
- If the harassment involves false statements that damage a person's reputation, the victim may pursue a **defamation claim**.

Further information and guidance

- For all questions and concerns: communications@bas.ac.uk
- For all media queries and collaboration suggestions: press@bas.ac.uk
- UKRI communications guidance
- Civil Service standards for social media
- GCS countering misinformation toolkit

Useful links

- Ofcom
- Code of Practice for online social media platforms GOV.UK
- Online Safety Act: explainer GOV.UK
- UK leads the way in a 'new age of accountability' for social media
- Social media playbook GOV.UK
- Social media guidance UK Government Security Beta
- CIPR Social Media Panel launches new Social Media best practice guide