

Frequently asked questions

These are provided for guidance or quick reference guide only, so always refer to and use in conjunction to the Social Media and Acceptable use Policy.

1. General Definitions

1.1 What is social media?

Social media is the term used to describe websites and online tools which allow users to share content and interact with each other.

1.2 What counts as a social media profile?

A social media profile is an account on a social media channel or platform that you control. This can be identifiable using your name and photo or anonymous using a handle/username. Social media channels include public platforms such as Facebook, Instagram, X, YouTube, TikTok, Snapchat, LinkedIn and forums such as Threads.

You should also apply this policy when using messaging tools such as WhatsApp and when creating websites and blogs.

Types of accounts:

Work-based Account

A work-based social media count must adhere to the Code of Conduct set out by NHS Blood and Transplant.

Personal Account

Your social media account including your name, handle, profile image and URL are your personal responsibility. Where an employee's connection to NHS Blood and Transplant is affiliated or apparent the centre you work in should not be included and a disclaimer is required on your profile/ bio such as, "The views expressed on this [social media account, blog, website] are my own and do not reflect the views of my employer."

1.3 What's the difference between externally facing social media and internally facing social media?

Externally facing accounts target the general public, customers, or clients, while internal facing accounts are restricted to employees or specific individuals within an organisation.

2. What are my responsibilities when using social media?

Your social media activities should be consistent with our high standards of professional conduct and in line with our organisational values (Caring, Expert and Quality):

- Be accurate, clear and honest in your communications.
- Be respectful and professional to fellow employees, business partners, competitors and patients.
- If in doubt seek guidance before posting.
- Direct donor queries/complaints/issues through the relevant channels, it is important we have a consistent approach and respond as an organisation rather than as individuals.
- You must not share confidential or sensitive information about NHS Blood and Transplant.
- You are responsible for keeping your accounts secure and for any content that is posted on your profiles.
- Always adhere to the rules of the platform you are using.

(Please see the [NHSBT Code of Conduct](#))

You must not:

- Create or transmit material that might be defamatory or incur liability to NHSBT.
- Post messages, photography, status updates or links to material or content that is inappropriate:
- Inappropriate content includes pornography, racial or religious slurs, gender-specific comments, information encouraging criminal activity or terrorism, or materials relating to cults, gambling, or illegal drugs.
- This definition of inappropriate content or material also covers any text, images or other media that could reasonably offend someone based on race, age, sex, religious or political belief, disability, sexual orientation or any other characteristic protected by the Equality Act 2010.

Use social media for any illegal or criminal activities.

- Send offensive or harassing material to others via social media.
- Publish unsolicited views on social, political, religious or other non-business-related matters.
- Use social media for advertising or endorsement purposes.
- Send or post messages or material that could damage NHSBT's image or reputation.

- Discuss colleagues, customer, patients, or suppliers without their approval.
- Post, upload, forward or link spam, junk email, chain emails and messages.

Inappropriate content covered in this policy includes the use of all languages. Whilst staff have a right to a private life and freedom of expression, as public servants all employees must avoid making any comment on their personal social media accounts which is likely to harm the security or reputation of the Employer. This applies to commentary on Government policy, service or directly on NHSBT as an employer.

Additionally, where an employee's personal social media profile identifies their association with NHSBT, care must be taken when posting content.

Unacceptable activity includes, but is not limited to:

- Making comments which deem abusive, offensive, obscene, vulgar or violent.
- Abusing, threatening, stalking, harassing or in any way attacking other users on the platforms.
- Posting any content that is offensive or derogatory toward others in regard to race/ethnicity, religion, gender, nationality or political beliefs.
- Using any language or content that is disruptive, repetitive, misleading, deceptive, unlawful or fraudulent.
- Trolling.
- Commercial solicitation.
- Uploading or attaching files that contain viruses, corrupted files, or any other similar software or programs that may damage the operation or compromise the security of computers and networks.
- Violations of intellectual property rights.

2.1 What responsibilities do I have when using social media as part of my role?

If you are using social media as part of your role this should have a clearly defined purpose and be in agreement with your manager. If your manager deems your use of social media unreasonable and unnecessary during your working hours, then this could lead to disciplinary action.

As an organisation who promotes NHS values of caring, expert and quality we expect this to be reflected in the behaviour and conduct of all communication including when using social media.

Report any issues or concerns encountered when using social media as part of your role.

2.2 What responsibilities do I have when using social media outside of work?

- It is vital to maintain confidentiality in regards to NHSBT especially when discussion of any sensitive or private information. The organisation must not be brought into disrepute.
- If you are talking about NHS Blood and Transplant, you should identify your role and connection with the organisation and make it clear you are not speaking on behalf of the organisation.
- Where your connection to NHS Blood and Transplant is apparent, you should include a disclaimer on your profile: "The views expressed on this [social media account, blog, website] are my own and do not reflect the views of my employer." Consider adding this in an "About me" or bio section of your social media profile or blog.
- Be aware of the risks using social media when you are under the influence of alcohol/ drugs.

3. Sharing concerns

3.1 What can I do if I see something concerning on social media, for example a donor issue or complaint or misinformation spreading?

If you see anything concerning on social media you, report this to the [social media team, socialmedia@nhsbt.nhs.uk](mailto:socialmedia@nhsbt.nhs.uk), as soon as possible. Please take a screenshot and note the link before escalating so the social media team can investigate.

3.2 What can I do if I am concerned about something a colleague has shared on social media?

If you are concerned about the welfare or conduct of a colleague, speak to your manager for advice. It is often easier to resolve situations offline directly with that person and signpost to support. Issues can be escalated to the social media team and HR Direct.

Staff complaints cannot be managed on social media and will be referred to the correct channels.

3.3 What do I do if I disagree with a social media post made by another team or on behalf of the organisation?

Disagreements and concerns are often better discussed and resolved offline and it is important not to get drawn into public disagreements or publicly criticise other teams or individuals, always be respectful and professional and report any concerns.

3.4 What do I do if my account is hacked?

You are responsible for keeping both your work and personal accounts secure, this includes using strong passwords, not sharing login details with others and logging out of accounts on shared devices.

If your account is compromised, change your passwords as soon as possible, report the issue to the platform and let the social media and cyber security teams know.

4. Getting involved

4.1 Can I request/ set up a work account/ channel for myself or on behalf of my team ?

If you will be using an account as part of your role this should be in agreement with your manager. You must get approval from the social media team, socialmedia@nhsbt.nhs.uk before setting up new accounts on behalf of the organisation including for teams and departments. It is important that all accounts adhere to platform rules and have a clear purpose, value and are properly managed.

Your social media name, handle, profile image and URL should not include NHS Blood and Transplant's name or logo. Where an employee's connection to NHS Blood and Transplant is affiliated or apparent the centre you work in should not be included and a disclaimer is required on your profile/ bio such as, "The views expressed on this [social media account, blog, website] are my own and do not reflect the views of my employer."

4.2 Do I need to use messaging apps such as Whatsapp to receive updates from my team?

Managers across the organisation use messaging apps such as Whatsapp to communicate messages and updates to their teams. It can be a convenient tool for quick and efficient communication among team members. However, this will not be the only form of communication. NHSBT uses various methods of communication to deliver messages. Please ensure your manager is aware which method of communication you are able to access.

4.3 What should I do if I'm approached to comment on behalf of NHSBT?

It is important for our reputation that individuals do not offer statements or comments on behalf of the organisation, especially around contentious issues. We need to have a consistent approach with signed off statements.

If you are approached to comment please contact the press office (pressoffice@nhsbt.nhs.uk).

4.4 Can I accept payment for posting something on social media?

Receiving payment in exchange for producing or posting social content could be a conflict of interest, speak to your manager in the first instance. Do not use any work social media accounts for advertising or promoting products or services.

4.4 Can I share images of my colleagues and donors on social media?

Always seek permission before sharing images or videos. You need to complete the model release form (please contact the Social Media Team for a form) when taking photos of donors and check the backgrounds of photos carefully in workplaces and donor centres to ensure nothing confidential is visible.

Always respect copyright and data protection laws.

4.5 Can Whatsapp and Social Media posts be requested under a Subject Access Request?

Subject Access Requests (SARs) refer to an individuals right to request their personal data that is held by an organisation. In the event a particular social media post or Whatsapp message in a work group chat can be disclosable as part of a SAR. In regard to social media posts this can also be referenced or requested.

5. Online abuse

5.1 What should I do if I receive abuse online?

Unfortunately, we are sometimes vulnerable to personal attacks or criticism on social media. Should this happen, speak to your manager initially to see if this can be resolved offline directly with that person, for example if it a known colleague, donor or patient.

Issues can be escalated to our social media team for advice and support with reporting to the relevant social media platform. It is important to take screen grabs and make links available so issues can be investigated. Please be aware the platforms will make the ultimate decision on removing content.

Any threats towards colleagues are taken extremely seriously by NHSBT, if you receive a threat it is important to report this to your manager, HR and the social media team. In rare and serious cases it may be necessary to report an incident to the police.

6. Policy Approval and Review

Policy version	UCD/People/Social Media/052v1.0/FAQsv1.0
Title	Social Media FAQ's
Approved by SPC	September 2023
EIA completed	November 2023
Counter Fraud check	10 October 2023
This document replaces	UCD/Comms/SM/001v1.0
Effective Release Date	November 2023
Review Date	November 2024
Author	Joanne Brown/Anna Taylor/Social Media Team
Filepath	G/HR/HR/Everyone/Policies
Distribution	All Staff and Managers; available on People First

7. FAQ's Section Details

Section	Section Heading	Page
1	General Definitions	1
2	What are my responsibilities when using social media?	2
3	Sharing concerns	4
4	Getting involved	5
5	Online abuse	6