



**Superior
Healthcare
Group**

Social Media Policy and Procedure

April 2026



Contents

1.	Background	3
2.	Purpose	3
3.	Scope	3
4.	General Principles	4
5.	Acceptable Use of Social Media	4
6.	Privacy, Confidentiality and Data Protection	4
7.	Professional Boundaries	5
8.	Reputational Risk and Conduct Outside Work	5
9.	Safeguarding and Reporting Concerns	6
10.	Training and Support	6
11.	Further Advice and Guidance	6

Version Control

Document Title	Social Media Policy and Procedure
Author	Name: Donna Cusack Job Title: Director of People and Development Email address: DonnaCusack@superiorhealthcare.co.uk
Last reviewed	April 2026
Last amended	April 2026
Next review due	April 2027

Version Details

Date	Version No	Status	Author	Reviewer	Approved By	Comments & Amendments
28.04.2026	0.1	Draft	Donna Cusack	LT		
30.01.2026	0.2	Minor amends	Donna Cusack	LT		
30.01.2026	1.0	Approved	Donna Cusack		ST	

Important Notice

This is a controlled document which is uncontrolled when printed. Please always access the latest copies of policies and procedures from The Superior Healthcare Group's Policies and Procedures Library stored on Microsoft Teams. If you do not have access to The Superior Healthcare Group's Policies and Procedures Library, please contact the author of this policy to confirm that it is the latest version using the contact details shown above.

Accessible Formats

In accordance with the Accessible Information Standard, this policy is available in alternative formats upon request, including large print or easy read. Employees and clients who require information in a specific format should speak to their Manager, Coordinator or the People Team.

1. Background

- 1.1 We recognise that social media can be a valuable tool for communication, learning, recruitment and engagement.
- 1.2 However, misuse of social media can place clients, employees, and the organisation at risk, particularly where confidential information is disclosed, professional boundaries are crossed, or reputational damage occurs.
- 1.3 There is an expectation that all employees will act professionally, respectfully and lawfully when using social media.

2. Purpose

- 2.1 This non-contractual policy sets out clear expectations regarding the safe and responsible use of social media by employees.
- 2.2 The purpose of this policy is to:
 - protect the privacy, dignity and safety of clients, families and employees.
 - maintain professional boundaries
 - reduce safeguarding risks
 - protect the reputation of the organisation
 - ensure compliance with legal and regulatory obligations
- 2.3 This policy supports compliance with the following CQC Quality Statements and Key Lines of Enquiry:

SAFE	Safeguarding and safe systems
WELL LED	Governance, management and sustainability
RESPONSIVE	Respect for individual need and communication preferences

- 2.4 This policy supports compliance with:
 - Malicious Communications Act 1988
 - Health and Social Care Act 2008 (Regulated Activities) Regulations 2014
 - UK GDPR and Data Protection Act 2018
 - Human Rights Act 1998
 - Care Act 2014
 - Equality Act 2010
 - Employment Rights Act 1996

3. Scope

- 3.1 This policy applies to all employees, workers, agency staff, contractors, volunteers and temporary staff.

3.2 It applies to use of social media:

- on company devices
- on personal devices where work is referenced
- during working hours
- outside working hours where conduct may affect the organisation, colleagues, clients or public confidence

3.3 Social media includes, but is not limited to: Facebook, Instagram, TikTok, X, LinkedIn, Snapchat, WhatsApp communities, YouTube, blogs, forums and messaging platforms.

4. General Principles

4.1 Employees must behave online in a way that is consistent with the organisation's values, Code of Conduct and professional standards.

4.2 Online conduct can have the same consequences as conduct in the workplace.

4.3 Employees remain personally responsible for content they post, share, comment on, like or repost.

4.4 Deleting content after publication does not remove responsibility for that content.

5. Acceptable Use of Social Media

5.1 Employees may use social media responsibly in their personal time provided this does not impact work performance, attendance or professional conduct.

5.2 Limited personal use during breaks may be permitted unless otherwise restricted operationally.

5.3 Employees must not present personal opinions as the views of the organisation.

5.4 Only authorised persons may post on behalf of the organisation or manage official company accounts.

5.5 Employees must also comply with the company's Email and Internet Usage Policy, IT and information security requirements, and any other relevant policies when using company devices, systems, email accounts, internet access or communication platforms.

6. Privacy, Confidentiality and Data Protection

6.1 Employees must never post, share or discuss confidential information relating to clients, families, staff or the organisation.

6.2 This includes names, photographs, addresses, care arrangements, diagnoses, routines, incidents, staffing matters or any information that may identify a person directly or indirectly.

- 6.3 Employees must not take photographs, videos or audio recordings in a client's home or workplace unless explicitly authorised in line with company policy and lawful consent requirements.
- 6.4 Employees must ensure privacy settings on personal accounts are reviewed regularly; however, privacy settings do not remove responsibility for content shared.
- 6.5 Employees should assume that any online content may become public.

7. Professional Boundaries

- 7.1 Employees must maintain clear professional boundaries with clients and their families.
- 7.2 Employees must not:
- add clients or family members as friends, followers or connections
 - accept friend requests from clients or family members
 - communicate with clients through personal social media accounts
 - use private messaging apps for care-related communication unless specifically authorised for business purposes
- 7.3 Any attempt by a client or family member to make personal contact through social media should be politely declined and reported to a manager.
- 7.4 Employees must not discuss personal relationships, grievances or conflicts involving clients or families online.

8. Reputational Risk and Conduct Outside Work

- 8.1 Employees must be mindful that personal online activity can affect the reputation of the organisation.
- 8.2 Employees must not post content that could reasonably:
- bring the organisation into disrepute
 - undermine trust in care services
 - cause offence to clients, families, colleagues or the public
 - amount to bullying, harassment or discrimination
 - promote hatred, violence or unlawful activity
 - suggest unsafe or unprofessional care practices
- 8.3 Serious breaches of this policy may be treated as gross misconduct and may result in dismissal without notice, depending on the circumstances. This may include, but is not limited to, breaches involving client confidentiality, safeguarding concerns, discriminatory or abusive content, unauthorised recordings, reputational damage, or serious breaches of professional boundaries.

9. Safeguarding and Reporting Concerns

9.1 Employees must immediately report any online content or behaviour that may indicate:

- abuse or neglect of a client
- exploitation or grooming
- discrimination or hate incidents
- threats of violence
- breaches of confidentiality
- conduct that places people at risk

9.2 Concerns must be reported to a line manager, safeguarding lead or through whistleblowing channels.

9.3 Safeguarding concerns may require referral to the Local Authority, CQC, police, DBS or professional regulators where appropriate.

9.4 Employees registered with a professional body, such as the NMC, must ensure their social media use is in line with their professional code. Care workers are also expected to follow the Code of Conduct for Healthcare Support Workers and Adult Social Care Workers in England.

10. Training and Support

10.1 Employees will receive guidance on professional boundaries, confidentiality and appropriate online behaviour.

10.2 Managers should provide additional support where concerns arise.

11. Further Advice and Guidance

11.1 Further guidance and support can be sought from the People Team at: Peopleteam@superiorhealthcare.co.uk