Social Media Policy

Controlled document - This document is uncontrolled when downloaded or printed

Document control							
Department		Finance				**Author**	Chief Financial Officer/ Head of Business Systems
Version	5	**Issued**	Jul 2023	**Review**	Jul 2025	**Audience**	Care UK Colleagues

Equality Impact Assessment Statement
As part of its development, this policy and its impact on equality have been reviewed as part of the ratification process. The purpose of the assessment is to minimise, and if possible remove, any disproportionate impact on residents or colleagues on the basis of age, disability, gender reassignment, race, religion or belief, sex, sexual orientation, marital or civil partnership status, pregnancy and maternity. No detriment was identified during the review of this policy.

1.0 Document Change Control

Version	Comments	Document Owner/ Approver	Issue Date	Review Date (2 years from issue)
1	First Issue – to reflect split of HC and RCS IT and ISMS management systems.	Finance and Commercial Director/ Head of IT and Business Systems	19.07.19	19.07.21
2	Second Issue – document owner added to title page. Document renumbered from CUK/ISMS/23 in the Group document set to CUK/RCS/ISMS/14 in the RCS set.	Finance and Commercial Director/ Head of IT and Business Systems	19.08.19	19.08.21
3	Third Issue – updated to reflect changes to business roles	Chief Financial Officer/ Head of Business Systems	31.07.20	31.07.22
4	Fourth Issue – new section 6.2 on use of social media for company use added, changes to commonly used social media platforms updated. Updated to new Care UK document template and branding.	Chief Financial Officer/ Head of Business Systems	31.07.22	31.07.24
5	Fifth issue - converted to WOW template. Document ref changed to CUKDREF10101, prev known as ISMS/014	Chief Financial Officer/ Head of Business Systems	31.07.23	31.07.25

2.0 Aim

Care UK recognises that colleagues may engage in electronic communication and internet usage during non-work time for purposes of personal interaction, recreation and self-expression using social media tools including, but not limited to, social networking sites, (such as Facebook, Instagram, Twitter, Whatsapp, LinkedIn, Glassdoor, Reddit), comments on newspaper or media web pages, blogs and other online journals and diaries, discussion boards and chat rooms, 3rd party rating sites such as Yelp, smartphone applications, multimedia host sites (such as YouTube, TikToc, Flickr, Pinterest, Tumblr, Vimeo) and similar media. Also, communication tools including Messenger, Snapchat, Zoom, Teams, and Skype are included in this policy, this includes electronic system-based communication channels used in Care UK at any given time. Collectively, this policy will refer to these as “social media”. The list is not exhaustive. As more sites, streams and channels come onboard these will fall under this policy by default.

This policy outlines where colleagues must ensure that their behaviour when using social media is not harmful to the organisation's reputation. Failure to adhere to this policy could lead to disciplinary action being taken.

This policy outlines the standards that Care UK requires colleagues to adhere to, the circumstances in which it will monitor instances and the action that will be taken in respect of breaches of these standards.

3.0 Objectives

This policy is not contractual. Care UK may vary or amend this policy at its discretion and may apply it as far as practicable in the circumstances.

4.0 Scope

This policy applies to all colleagues working at all levels and seniority, including all managers, colleagues (whether permanent, fixed-term or temporary), consultants, contractors, trainees, seconded staff, home workers, bank workers casual workers and agency staff, volunteers, interns, agents, sponsors, or any other person associated with us, or any of our subsidiaries or their colleagues, wherever located.

5.0 Responsibilities

5.1 Line Managers are Responsible for

- Ensuring they have full understanding of this policy and bringing it to the attention of colleagues in their work area.
- Ensuring colleagues are aware of their responsibilities about this policy and are aware of the consequences of not adhering to it.
- Actively addressing and resolving any misuse of social media.

5.2 Colleagues are Responsible for

- Ensuring they have read, understand and comply with this policy.
- Adhering to the principles of this policy.
- Reporting any incidents of misuse of social media that they are aware of to their Line Manager in a timely fashion.

5.3 The HR Function is Responsible for

- Advising Line Managers on the application of this policy.
- Providing advice to Line Managers where there are breaches of this policy.

6.0 Policy

Care UK does not intend to infringe on colleagues' personal lives or unnecessarily regulate colleagues' off-duty conduct. Nevertheless, there are situations when the personal use of social media can have a harmful impact on the company.

There is a clear professional and reputational risk if company information and/or sensitive resident and colleague personal data, referred to in comments and/or photographs posted on line, are used inappropriately or without due consideration of the risks involved.

The risks associated with any confidential or sensitive information being disclosed or anything which easily identifies Care UK`s working environment could lead to several outcomes:

- The individual is in breach of confidentiality;
- The individual could be committing a criminal offence under the Data Protection Act 2018;
- The individual may be in breach of Equality and Discrimination laws;
- The individual may bring Care UK`s name into disrepute;
- The individual may be prosecuted by the Information Commissioner (ICO).

In addition, when a colleague identifies themselves in a public forum as being affiliated with Care UK, whether intended or not, the colleague's online behaviour could be seen as a reflection of Care UK, even if the postings are not directly related to their employment.

6.1 General Principles

The following principles apply to all personal use of social media sites. Colleagues must follow all applicable policies regarding conduct; these apply equally to online and social media activities as they do to in-person behaviour i.e., colleagues must also abide by all Care UK policies (including, but not limited to):

- Dignity at Work Policy;
- Anti-Corruption Policy;
- The NMC's 'The Code' and Social Work code (of ethics and conduct);
- Computer Use Policy (includes email and internet use).

Care UK provides IT computing resources to its colleagues to conduct business activities. Limited personal use of the computing resources is tolerated if this is during break times, in a manner that is consistent with other general internet use and does not interfere with business activities or commitments. This applies to both computers and mobile devices.

Care UK does not allow the use of personal mobile devices and therefore the provision of access to social media sites whilst on duty, except in specific operational roles for which explicit line manager authorisation will be given.

Care UK reserves the right to request that inappropriate comments made by colleagues in the public domain on social media sites are removed.

Care UK reserves the right to selectively block access to specific internet sites on its network.

Colleagues may not disclose, confidential or sensitive information belonging to Care UK, or residents and their representatives or colleagues personal data, at any time on social media sites. Colleagues must always protect all confidential and sensitive information.

It is not appropriate for colleagues to connect with customers on social media sites because of the conflict of interest that this could cause.

Colleagues must not take photographs or note personal data of residents and colleagues on their personal devices (including mobile telephones, tablets).

Colleagues may not use or display the Care UK logo`s, trademarks or copyrighted materials on personal websites or elsewhere on their personal social media accounts. Colleagues should also respect all other parties copyrighted and intellectual property rights.

When using social media for personal use, colleagues are not authorised spokespersons of Care UK. If colleagues identify themselves as colleagues of Care UK, readers may incorrectly assume that they are speaking on its behalf. Therefore, if colleagues choose to refer to Care UK or their employment with Care UK in a personal blog or website, they must notify readers that the views, opinions, ideas and information being presented are their own personal views or opinions and are not in any way attributable to Care UK.

When topics relating to Care UK arise, colleagues should ensure that they follow all Care UK policies and carefully consider whether it is appropriate for them to comment. Colleagues are not authorised to covertly advocate for Care UK and failing to identify themselves as Care UK colleagues could mislead readers.

6.2 Permitted Use of Social Media for Business Purposes

The following specific instances are where social media usage is pragmatically permitted:

- Colleagues may share that they work for Care UK on social media accounts and are encouraged to share positive stories, news and events about the Company and the colleague's involvement. Colleagues must remember this makes them identifiable as working for the Company on the social media platforms used (use of Facebook and LinkedIn are common examples of this).

- Home Managers or supervisors may contact colleagues via WhatsApp to pass on company or home business information e.g., available shifts, communicating with individual or groups of colleagues. This must not be used by all parties to disclose any resident or colleague personal data e.g. name, clinical or medical information. It is envisaged this use will cease with the introduction of Care UK`s communication tool from the summer of 2023.

Homes manage and update their own Facebook account and hence must follow Care UK guidelines as to its usage as directed by the Marketing Department.

6.3 Breaches of this Policy

All colleagues are required to adhere to this policy. Colleagues should note that any breaches of this policy may lead to disciplinary action. Behaviour whilst using social media that is harmful to Care UK or acts of harassment or intimidation, are both examples of Gross Misconduct and may lead to dismissal.

Managers who become aware that a colleague has acted in breach of this policy have a duty to investigate the matter promptly and thoroughly and to take corrective and/or disciplinary action. Equally, if a colleague complains (whether informally, via the Whistleblowing process or through the Company's formal grievance procedure) about a colleague's conduct in respect of this policy, the manager should take prompt action to investigate and resolve the matter, addressing any behaviour that breaches the policy. It may be necessary in more extreme cases to instigate the formal disciplinary procedure and/or invoke the bullying and harassment procedure. The HR Department will assist any manager in dealing with breaches of this policy.

7.0 Evaluation Measures

7.1 Monitoring

Compliance to the processes and guidance contained within this policy will be highlighted through notification of any Information Security and other Information Governance breaches whereby an investigation will identify non compliance and then seek to understand and address the reasons for non compliance.

7.2 Audit and Review

Compliance to the processes and guidance contained within this policy will be highlighted through notification of any Information Security and other Information Governance breaches whereby an investigation will identify non-compliance and then seek to understand and address the reasons for non-compliance.

7.2.1 Internal Review

Compliance with this Information Security Policy will be monitored through IMS and Quality and Governance Internal Audits, and by other management checks as required.

7.2.2 External Review

Inspections by external auditors representing regulatory bodies, or by the regulators themselves, may be carried out from time to time at Care UK service delivery sites. These include:

- Care Quality Commission/Care Inspectorate Scotland/ Wales (under the terms of the Health and Social Care Act)
- Local Authorities (Environmental Health, Food Hygiene)
- British Standards Institute (as part of Care UK's ISO 27001/20000 certification)
- Health and Social Care/ Legal Regulators (DHSC, NHS Digital, ICO)

- Service Commissioners (NHS Bodies, Local Authorities)

As part of these activities, external inspectors may ask to view service user records and related information relating to the provision of care. Services should provide supervised access to view such records where requested.

Copies of corporate and service user records should not be removed from site by the inspector, unless this has been specifically approved by an authorised manager.

8.0 Review

This Policy is reviewed by the Information Governance Steering Group at regular intervals, not exceeding two years.

9.0 Distribution

All Care UK colleagues, via mycareuk.com.

10.0 Reference Documents

10.1 Care UK Policies, How to Guides and Supporting Documents

Related Policies	
ISMS	
1	Information Security Management System Overview
2	Information Governance Policy
3	Information Security Policy
4	Information Control Policy
5	Information Classification Guidelines
6	Information Security Incident Reporting Policy
7	Data Protection Policy including Caldicott and Confidentiality Principles
8	Data Protection Impact Assessment Process
9	Computer Use Policy
10	Mobile Device Acceptable Use Policy
11	Bring Your Own Device Acceptable Use Policy
12	IT Asset Lifecycle and Disposal Policy
13	Information Security Awareness Guide / Presentation
14	IS Risk Assessment and Management Procedure
15	Physical Security Policy
16	Visitor Policy
17	Subject Access Request Policy
18	Social Media Policy
19	IT Systems Logical Access Control Policy and Process
20	Clear Desk and Screen Policy
21	Information and Data Exchange Protocol

22	Information Sharing Agreement Template
23	Secure Email Process
24	Fax Management Procedure
25	Third Party Supplier Approval and Management Policy
26	Third Party Contracts Guidance and Confidentiality Policy
27	Secure Development Policy
28	Secure Systems Engineering Principles Guidance
29	Service Decommissioning Process
30	Service Decommissioning Planner
31	IT Backup and Restore Policy and Process
32	IT Logging and Monitoring Policy and Procedure
33	Applicable Legislation List
34	ISO 27001 Statement of Applicability
35	Business Continuity Plans
IMS	
1	Records Management Policy
2	Records Retention Schedule and Archiving Policy
3	IMS Internal Audit Procedure
4	Corrective and Non-Conformance Process
5	IMS Communications Policy and Plan
IT SMS	
1	IT Service Management Plan
2	IT Change Control Policy and Process
3	Cyber Security Incident Response Process

Related How to Guides	
1	N/A

Related Supporting Documents	
1	N/A

10.2 External Regulation and Legislation

Care UK is bound by the following legislation and compliance standards listed below that governs the handling of Person Identifiable Information:

- UK Data Protection Act 2018
- General Data Protection Regulations
- Health and Social Care Act 2012
- Human Rights Act 1998 (Article 8)
- The Common Law Duty of Confidence.

Related External Reference Documents	
1	NHS Digital Data Security and Protection Toolkit
2	ISO 27001 (Information Security Management Standard)

3	ISO 20000 (IT Service Management Standard)
4	Information Commissioner Guidance
5	Information Governance Alliance Guidance

Please note: All appendices referred to in this policy can be found on mycareuk.com

CUK/ISMS/14