

Policy

Social Media policy.docx

7 May 2024

NR/HR/POL/029

Contents

The policy	3
1 Introduction	3
2 Scope	3
3 Social media	3
4 The Use of Company Property & Equipment for Personal use of Social Media	4
5 Using social media platforms in Network Rail's name	4
6 Using social media to share work related content.....	5
7 Recruitment.....	6
8 Privacy on Public Forums	6
9 Rules for use of social media, including for private use.....	6
10 Monitoring	8
11 Breaches of this policy	8
12 Reporting Breaches of this Policy	8

The policy

1 Introduction

1.1 Social media platforms are increasingly used as a means of communication both at work and at home. This policy outlines the standards we require employees to observe when using social media, the circumstances in which we will monitor use of social media and the action we may take if this policy is breached. This policy should be read in conjunction with our Acceptable Use Policy which can be found here: [Acceptable use of information and information systems Policy.docx \(sharepoint.com\)](#) which sets out how Network Rail's internet and email systems and networks can be used and also the Bullying and Harassment Policy and Procedure, and the Privacy and Data Protection Policy which are available on MyConnect.

2 Scope

2.1 This policy applies to all those working for Network Rail including employees, agency workers, contractors, and other third parties working for Network Rail, for example secondees, (referred to collectively as 'employees' in this policy).

2.2 All employees are expected to have read and adhere to this policy.

2.3 This policy does not seek to regulate the use of social media in a purely private capacity where that use has no bearing on Network Rail or its activities. It is intended to outline the rules governing the use of social media when referencing Network Rail, or where the use of social media may affect Network Rail or our activities. It is designed to help Employees use these platforms and services responsibly, to minimise the risks set at 3.3 and to apply consistent standards of use of social media. If there is any doubt that any content posted on social media by an employee could affect the reputation of Network Rail, they should consider whether to post at all.

This policy applies where:

2.3.1 The use of social media relates to Network Rail or its activities;

2.3.2 The use of social media relates to, or is otherwise connected with, an employee's, contractor's or agency worker's role or work at Network Rail whether the intended use is personal or professional;

2.3.3 A person is identifiable as someone employed by, or otherwise associated with, Network Rail.

3 Social media and its use

3.1 In this policy, 'social media' means internet-based applications which allow users to collaborate or interact socially by creating and exchanging content, such as social networks or platforms, community sites, blogs, microblogging sites, wikis, web forums, social bookmarking services and user rating services. Examples include, but are not limited to Facebook, LinkedIn,

YouTube, Instagram, X, WhatsApp, TikTok, Spotify, Snapchat, Tumblr, Flickr, SlideShare, Pinterest and Viva Engage.

- 3.2 Key business decisions must be recorded on Network Rail's systems, for example email and Microsoft Teams, social media platforms should not be used to record decisions.
- 3.3 Improper use of social media may result in the following:
- A breach of the employee's employment contract, or a breach of the terms and conditions of the agreement that exists between an agency worker or with any contractor;
 - A breach of our policies;
 - A breach of data protection legislation;
 - Misuse of confidential information or that of our customers and/or suppliers and/or reputational damage;
 - Claims of libel and defamation (i.e. damaging the good reputation of another person or organisation), that can lead to civil court cases where an injured party seeks the payment of damages as redress.

4 The Use of Company Property & Equipment for Personal use of social media

- 4.1 Company devices, such as laptops and mobile phones are the property of Network Rail and must be returned to Network Rail if and when requested.
- 4.2 Email addresses that end in "@networkrail.co.uk" (or Microsoft variants) or are identifiable or connected to Network Rail such as group names, alliances, joint ventures etc are the property of Network Rail and should only be used for work purposes or limited personal use in accordance with the Acceptable Use Policy. Employees must not use work email address to sign up for personal use of social media platforms. The only exception is on the Network Rail's Viva Engage site or where it is necessary for your role, for example HR colleagues often advertise roles via platforms such as LinkedIn.
- 4.3 Permission to use Network Rail systems to access social media platforms for personal or work use may be withdrawn at any time at Network Rail's discretion.

5 Using social media platforms in Network Rail's name

- 5.1 Only the authorised communications and resourcing teams are permitted to post in Network Rail's name or on Network Rail's behalf and using Network Rail's logo and branding. They are permitted to post on any of Network Rail's official pages on social media platforms on behalf of Network Rail. This includes accounts or presences that aim to showcase specific Network Rail projects or schemes with own branding; even if not using the Network Rail logo, this still constitutes representation of Network Rail and is bound by the same rules. Any breach of this restriction may be treated as gross misconduct.

5.2 Employees are not permitted to represent Network Rail in social media unless this is part of their role at Network Rail, or they have the written permission from the Group Communications team or an appropriate senior manager of the business.

5.3 Any employees required to use social media to represent Network Rail must complete the required 'Social Media Governance at Network Rail' e-learning.

6 Using social media to share work related content

6.1 Network Rail recognises the importance of social media platforms in shaping public thinking about Network Rail, our services, employees, customers and other business partners. We also acknowledge that our employees have an important role to play in shaping industry/sector conversation and direction through interaction in social media.

6.2 Employees are able to interact on social media platforms, such as LinkedIn about the rail industry/sector if the information is already publicly available or, if not, if the information has been approved by the communications team to share externally.

6.3 Any information shared on a public platform should never compromise safety or the operation of the railway. This includes, but is not limited to, posts which reveal operation code names, code words, call signs, access credentials (physical or IT), plans, screen shots of sensitive information, photographs etc. It is important to check any posts before posting to make sure there is nothing in them which will compromise safety or security. For example, photographs could have information in the background which present a risk. If you are not sure do not post and check with the data owner whether it can be shared.

6.4 Network Rail recommends that Employees disassociate themselves from sites/ groups if they believe the nature of those sites or conversations is becoming inappropriate – do not get drawn in and if you have a concern raise it with your line manager or submit via Speak Out.

6.5 When undertaking permitted work-related social media interaction, Employees must:

6.5.1 clearly identify themselves, including name and job title, if it will be attributed to them as part of their role. It is important that posts are clear that the views are their own and do not necessarily reflect Network Rail's views. It is recommended that the following disclaimer is used: 'The views expressed are my own and do not necessarily reflect the views of my employer'; you could add this disclaimer to any posts connected to Network Rail or your bio on that platform;

6.5.2 communicate in a professional manner, using non-offensive language and be accurate and appropriate for the intended audience;

6.5.3 not provide references or recommendations for anyone else on social media (whether employment or business recommendations) in any way that suggests any endorsement or recommendation by Network Rail;

6.5.4 if you become aware of adverse criticism of Network Rail or of content you have created or shared, do not respond. Inform your line manager, and escalate to either regional comms team if you are based in a region or national team if you are in a central function;

6.5.5 comply with the terms and conditions and policies of the social media platforms you use;

6.5.6 maintain good information security practices. Use strong passwords and make appropriate use of security and privacy settings on social media platforms, and follow our email, internet and communications and information security policy, guidelines and standards.

7 Recruitment

7.1 We may carry out vetting of an employee's personal or business-related platforms where necessary to protect Network Rail's legitimate interests, for example, where an employee is undertaking a voluntary role within the business which is public facing or if an employee is being put forward for an honour or other recognition by Network Rail. Where we do so, searches will be conducted in accordance with data protection laws.

8 Privacy on Public Forums

8.1 Social media is a public forum. Therefore, there should be no expectation of privacy or confidentiality in anything you create or share on social media platforms. When you create or exchange content using social media you are making a public statement. As such, your content will not be private and can be shared, screenshot, copied or forwarded to third parties without your consent. You must therefore consider the potential sensitivity of disclosing any information, including personal or other sensitive information (such as health information or your place of work) on a platform, and work on the basis that what you write, and share will be shared with multiple people. Once sensitive or confidential information (or offensive or defamatory information) has been disclosed, it can never be recovered, and this may impact Network Rail and/or third parties and you personally.

8.2 You should be wary of posts to 'private' areas or areas behind 'walls'. Other members may make your posts 'public'. Some private areas have memberships almost as large as public memberships. Posting content that breaches this policy on a private forum is subject to the same rules as a public forum.

8.3 You should regularly review the privacy and data collection settings on your personal social media accounts and appropriately restrict the people who can read your comments. Review the content of your personal social media accounts on a regular basis and delete anything that could reflect negatively on others on you in a professional capacity or on Network Rail.

9 Rules for use of social media, including for private use

9.1 Employees have a right to a private life and freedom of expression however there can be an overlap between work life and private life when interacting on social media platforms, particularly where you can be identified as working for Network Rail. All employees must

respect copyright, fair use, data protection, defamation, libel and financial disclosure laws and must avoid making any comment on personal social media accounts which is likely to harm the security or reputation of Network Rail and/or any of our employees.

9.2 When creating or exchanging content on a social media platform including when this is for personal use, you must at all times comply with your contract of employment (or other contractual relationship) with Network Rail, all rules and any of our policies that may be relevant. In particular you must not:

9.2.1 bully, harass or victimise any employee, worker, customer, third party or other person associated with Network Rail, and/or breach our Bullying and Harassment Policy and Procedure;

9.2.2 discriminate against any employee, worker, customer, third party or other person associated with Network Rail;

9.2.3 breach Network Rail's data protection or information security policies;

9.2.4 Use private groups, for example, Whatsapp, to make work related decisions or approvals;

9.2.5 actually, or potentially, bring Network Rail or its name into disrepute.

9.2.6 divulge any confidential information and respect any confidentiality obligations owed by you or Network Rail;

9.2.7 disclose commercially sensitive material or infringe any intellectual property or privacy rights of Network Rail or any third party;

9.2.8 make defamatory or disparaging statements about Network Rail, its employees and other workers customers or suppliers. If you see such comments please immediately inform your line manager;

9.2.9 create or share or link to abusive, obscene, discriminatory, derogatory, defamatory or pornographic content that can be linked or perceived to be linked to Network Rail in any way;

9.2.10 upload, post or forward content such as screen shots or photographs which could create a safety risk, belonging to another company or person unless you have their consent;

9.2.11 speak or post anything on behalf of Network Rail unless it is within the confines of your role, or you have been provided with written authorisation to do so.

9.3 Where a post may be connected to Network Rail, you should be mindful of the impact your posting on a social network or platform may have on the perception of Network Rail.

9.4 If you make a mistake in a posting, be prompt in admitting and correcting it. Where you have or believe you may have breached any company rule or policy, you should inform your line manager, and where appropriate declare this on iEthics.

The Information Security team has created social media guidance to support when posting on behalf of the company which can be found here: [Communications - social media policy](#).

You can also find guidance for using social media effectively here: [Social media guidance](#).

10 Monitoring

10.1 Network Rail reserves the right to monitor how its information systems and equipment is used and this includes the reading and monitoring of all messages, posts, tweets etc, and includes all social media entries that are received, viewed or sent using Network Rail systems and equipment.

10.2 Anyone suspecting misuse of social media can report instances to their regional or central social media/communications team or through Network Rail's confidential 'Speak Out' service Network Rail will review Speak Out complaints and respond appropriately.

11 Breaches of this policy

11.1 We consider this policy to be extremely important. If an employee is found to be in breach of the policy, they may be disciplined in accordance with the Disciplinary Policy and Procedure and/or Bullying and Harassment Policy as appropriate. Breaches of this policy may be considered gross misconduct, which may lead to summary dismissal with the termination of employment without notice or payment in lieu of notice.

11.2 If a contractor, consultant, agency employee or other worker is found to be in breach of the policy, the matter will be reported and managed in line with your contractor's or employment agency agreement. In certain circumstances, breaches of this policy may result in you ceasing to work for Network Rail.

11.3 In addition, you should note that in certain circumstances, for example where a post is deemed to be seditious or inciting violence against passengers or employees or damage to Network Rail property, it could lead to an investigation under the Sentinel Rules and in serious cases may lead to the removal of your Sentinel card and access to work on Network Rail infrastructure.

11.4 Employees should note in particular that creating or sharing content on a social media platform may, depending on the content, amount to gross misconduct even if it takes place:

11.4.1 on a personal account;

11.4.2 outside working hours;

11.4.3 without using our computers, systems and networks; and/or

11.4.4 within a social media group or forum that identifies as 'private' 'closed' or similar because once something has been posted it can be shared further than these groups.

11.5 In certain circumstances, an act that breaches this policy may also constitute a criminal offence, or could lead to a civil claim being made against the individual for example in defamation.

11.6 In addition to any actions Network Rail may take in relation to breaches of this policy, the laws that were in existence prior to the development of social media regarding written material that is published, for example, libel, defamation, harassment, discrimination, threatening violence and sedition, etc. will normally applies to posts on social media, and can in some circumstances lead to criminal or civil proceedings.

12 Reporting Breaches of this Policy

12.1 If, in the course of using social media, you become aware of any misconduct or wrongdoing by any employee, officer, worker or agent of Network Rail, you must report it to your line manager in the first instance or submit via Speak Out.

12.2.1 You may be required to remove content created or shared by you which we deem to be in breach of this policy. Refusal to comply with any reasonable request to remove content deemed to be in breach of this policy, will be considered as a failure to comply with a reasonable request, and may lead to disciplinary action.

12.3 Employees who feel that they have been harassed or bullied because of material posted or uploaded by a colleague onto a social media platform should inform their line manager or HR in accordance with our Harassment Policy and Procedure.

Document control

Version	2.00	Document	Social Media policy.docx
Supersedes	1.00	Reference	NR/HR/POL/029
Date created	17/11/2021	Author	Tamara Hill, HR Policy Manager
Date approved	2 May 2024	Owned by	Employee Experience
Implementation date	07/05/2024	Approved by	Tracy Macnicoll, HRD Employee Experience

Version control

Issue	Date	Remarks/Comments
1.0		Policy pulled forward from 2021
2.0	May 2024	Reviewed 1.2 If there is any doubt that any content posted on social media by an employee could affect the reputation of Network Rail, they should consider whether to post at all. 3.1 Examples include, but are not limited to Facebook, LinkedIn, YouTube, Instagram, X, WhatsApp, TikTok, Spotify, Snapchat, Tumblr, Flickr, SlideShare, Pinterest and Viva Engage. 5.1 Only the authorised communications and resourcing teams are permitted to post in Network Rail's name or on Network Rail's behalf and using Network Rail's logo and branding. They are permitted to post on any of Network Rail's official pages on social media platforms on behalf of Network Rail. This includes accounts or presences that aim to showcase specific Network Rail projects or schemes with own branding; even if not using the Network Rail logo, this still constitutes representation of Network Rail and is bound by the same rules. Any breach of this restriction may be treated as gross misconduct. 6.5.2 communicate in a professional manner, using non-offensive language and be accurate and appropriate for the intended audience; 6.5.4 if you become aware of adverse criticism of Network Rail or of content you have created or shared, do not respond. Inform your line manager, and escalate to either regional comms team if you are based in a region or national team if you are in a central function;

		7.1 We may carry out vetting of an employee's personal or business-related platforms where necessary to protect Network Rail's legitimate interests, for example, where an employee is undertaking a voluntary role within the business which is public facing or if an employee is being put forward for an honour or other recognition by Network Rail. Where we do so, searches will be conducted in accordance with data protection laws. 8.2 You should be wary of posts to 'private' areas or areas behind 'walls'. Other members may make your posts 'public'. Some private areas have memberships almost as large as public memberships. Posting content that breaches this policy on a private forum is subject to the same rules as a public forum. 9.4 If you make a mistake in a posting, be prompt in admitting and correcting it. Where you have or believe you may have breached any company rule or policy, you should inform your line manager, and where appropriate declare this on iEthics. The Information Security team has created social media guidance to support when posting on behalf of the company which can be found here: Communications - social media policy. You can also find guidance for using social media effectively here: Social media guidance. 12.1 If, in the course of using social media, you become aware of any misconduct or wrongdoing by any employee, officer, worker or agent of Network Rail, you must report it to your line manager in the first instance or submit via Speak Out.
--	--	---