Social Media Protocol
(Personal and Trust Business Use)

1.0 Protocol Statement

1.1 This protocol applies to personal and approved business use of social media. The Trust recognises that social media plays a part in everyday life and supports the responsible use by its employees, but care needs to be exercised with its use, hence the need for the following protocol.

1.2 The term social media covers IT based technologies (desktop, laptop, tablet and smartphone) that allow the creating and sharing of information, ideas, career interests and other forms of expression in a public forum via virtual communities and networks.

1.3 The Trust recognises that staff may wish to engage with social networking sites. Whilst it is recognised that all employees are entitled to privacy in their personal life, the Trust is committed to maintaining confidentiality and safety at all times whilst also maintaining the reputation of the Trust, the wider NHS and of the relevant profession by displaying acceptable behaviour at all times.

1.4 This protocol is not meant to deter employees from using social media for personal or business use but is necessary to protect employees and prevent them from bringing the NHS into disrepute, either inadvertently or intentionally, and inform them of the potential consequences of doing so.

1.5 All employees must be aware that, even if they believe that they are using these sites with enhanced privacy settings applied, this does not exempt them from the guidelines outlined in this protocol.

1.6 If employees have concerns about the online conduct of any other employee this must be raised with an appropriate manager in the first instance; however if employees are not comfortable in doing so, they can raise concerns in accordance with the Trust's HR06 – Dispute Resolution in the Workplace Policy and the HR 16 – Trust's Raising Concerns at Work Policy (where staff wish to raise a concern through a protected public interest disclosure i.e., a 'whistle blow').

1.7 All staff must ensure that any information shared for Business Use on Social Media is compliant with the General Data Protection Regulations (GDPR). Any requests relating to Individual Rights (the right to; Access, Rectification, Erasure, Restrict Processing, Data Portability, Objection and in relation to Automated Decision Making) will be processed in accordance with the OP07 – Trust's Health Records Policy and HR09 – Employee Records Policy.

2.0 Definitions

Social media is the term commonly used for web-based and other mobile communication technologies that enable message and opinion to be shared in dialogue with other who often share the same community interests. Social media

allows users to connect with each other, including sharing statement, photos, videos and live streams and can also be used to gather information, opinion or donations from members of the public. It may be access through an internet browser or an application (app). Popular platforms include, but are not confined to:

Facebook
WhatsApp
Messenger
Tumblr
Instagram
Pinterest
LinkedIn
Snapchat
Twitter
YouTube
TikTok
Vimeo

3.0 Accountabilities

3.1 The **Director Sponsor (Chief People Officer)** will be accountable for the revision of this protocol which is necessary from time to time as a result of changes in the law or in the light of experience when applying the protocol.

3.2 **All managers** will be responsible for ensuring that this protocol is fairly and consistently applied within their area of responsibility in the Trust.

3.3 **Employees** will be responsible for complying with this protocol and the Trust's Standards of Behaviour and Conduct at all times.

4.0 Procedure Detail

4.1 General Principles

4.1.1 Employees must ensure that whilst utilising social media sites, they adhere to high professional standards of behaviour. This protocol sets out the principles for the use of social media **for personal and business use.** Many people now expect to use social media to interact with each other, and with service providers. The protocol aims to protect employees and prevent them from bringing the Trust and /or wider NHS into disrepute either inadvertently or intentionally.

4.1.2 This protocol applies to all staff, including those working via honorary contracts, secondment contracts, visiting clinical staff, sub-contractors, bank and agency workers, volunteers, apprentices and students working on Trust premises.

4.2 Use of Social Media at Work for Personal Use

4.2.1 Employees must limit their personal use of social media on Trust computers or devices to allocated break times only. Internet use is logged and monitored as per OP12 – IT Security Policy. The Trust is aware that employees may wish to bring their own devices such as mobiles and other hand-held devices to access social media websites whilst they are at work. **Employees must limit their use of social media on their own equipment to allocated break times only.**

4.2.2 If an employee states on social media platforms that they work for the Trust, they must be aware of the potential risks associated with this for example members of the public may be able to search for and identify an employee's work location. Adjusting your privacy settings on a social networking site will restrict who can access your profile and will therefore prevent members of the public from finding out personal information about you. Please refer to Appendix 1 – How to check your Facebook Privacy Settings in less than 10 minutes for guidance on how to check your Facebook privacy settings are protected.

4.2.3 If an employee chooses to identify that they work for the Trust on a personal social account, they must be aware that members of the public may associate their personal thoughts, actions and behaviours with the Trust and indeed the wider NHS. Stating that, for example 'all my thoughts are my own,' will not safeguard staff against this. Any comments made on social media about colleagues, managers or patients have the potential to be linked to the workplace.

4.3 Personal Use of Social Media

4.3.1 Whilst using social networking sites for personal use employees must be aware of the image they present online and manage this proactively. The Trust recognises that social media plays a part in everyday life and supports the responsible use by its employees, but care needs to be exercised with its use. Used properly, social networking sites such as Facebook are a great way to find old friends, join interest groups and share information. However, staff must remember that anything posted on a social networking site is in the public domain.

4.3.2 Staff must recognise that there is a clear relationship between conduct in the real world and conduct online. The Trust has a clear policy on staff rules relating to standards of behaviour and conduct (Trust's Disciplinary Policy HR03 – Attachment 1) and there is an expectation that online conduct must be at a similar high standard.

4.3.3 Remember everything posted online is public, even with the strictest privacy settings. Once something is online, it can be copied and re-distributed, and it is easy to lose control of it. Presume everything posted online will be permanent and will be shared.

4.3.4 Staff must recognise that they can bring the Trust into disrepute and damage its reputation.

When using social media staff <u>MUST NOT</u>:

- *Bring the Trust into disrepute* – for example making and/or endorsing defamatory comments about any individuals, organisations, groups, employees or criticising or arguing with service users connected in any way with NHS service provision.

- *Breach confidentiality* – this includes breaching the confidence of patients and staff. Information which could identify patients or service users must not be released: examples include demographic information (name, age and address), diagnosis, ward or area seen (for example ED or outpatients). Confidential information about staff members must also be protected (this includes information about sickness absence and job roles); unless the staff member has already made the information public knowledge. If you are unsure of whether to publish something, please refer to your line manager or the Trust's Information Governance Policies.
- *Breach the Trust's Commercial Interests* – information about the Trust's business must not be published via social media, this includes information about partner organisations, contracts and internal processes. The Trust will manage the publication of its information through appropriate channels. If you are unsure of whether to publish something, please refer to your line manager or the Trust's Information Governance Policies.
- *Breach Trust Copyright* – by using Trust images or written content without their permission, or by failing to give acknowledgement where permission has been given (unless re-sharing a post that the Trust have made public, i.e., for example, re-sharing on Facebook or re-tweeting on Twitter).
- Publish images or make comments that:
  - Are considered as bullying, harassment, inflammatory or intimidating in nature.
  - Are of a discriminatory, offensive or inappropriate nature. This includes the promotion of discrimination-based factors such as race, sex, religion, nationality, disability, sexual orientation or age.
  - May create a security risk for the Trust.
  - Contain confidential and/or sensitive information; this includes images of Trust information and patients. When posting any images within the workplace, care must be taken to ensure that no personal identifiable or confidential information is shared. Images of staff members posted onto social media sites must be done with their prior consent.
  - Are about patients and/or service users on social media. This includes forums such as; WhatsApp groups or Facebook Messenger, even if the forum is private amongst colleagues.
  - Are considered slanderous, defamatory, obscene, indecent, lewd, pornographic, violent, abusive, insulting or threatening.
- Use the Internet in any way to attack or abuse colleagues, patients or service users.
- Use social media to promote or assist in any unlawful act.
- Use their NHS email address or contact details to set up their social media or advertise this as a contact address within the social media site.
- Use NHS logos within the site that may give the impressions of official endorsement.
- Use the identity or likeness of another employee, contractor or service user.

- Imply you are authorised to speak on behalf of the Trust.
- Provide professional medical advice through the use of social media.
- Use social media for publicly raising or escalating concerns

This list is not intended to be exhaustive. If there is any doubt about whether a particular activity online is acceptable, it can be useful to think through a real-world analogy. For example, manipulated photos that are intended to mock individuals would be considered offensive if printed and pinned on workplace notice boards, and are no less offensive when shared online, even when privately shared between friends.

4.3.5 It is not advisable to befriend patients, relatives or carers on social networks, particularly if you use social networks to reveal aspects of your personal life. If a patient contacts you about their care or other professional matters through a personal profile, it is recommended that you indicate that you cannot mix social and professional relationships see Relationship at Work Guidance. In addition to this Trust guidance, professionally registered staff must adhere to any social media guidelines provided by their registering bodies as per section 4.0 of this protocol below.

4.3.6 Staff must be aware of the consequences of using social media sites to post any content that conflicts with information that they have already provided to the Trust, for example in relation to their health and fitness for work or any secondary employment that they undertake. These actions will bring about possible disciplinary proceedings in line with the Trust's Disciplinary Policy (HR03) and referral to the Trust's Counter Fraud Specialist via the Anti-Fraud and Corruption Policy (GP02).

4.4 Professional Registration and Social Media

4.4.1 Professionally qualified staff will put their registration at risk if they fail to adhere to the guidelines above. Professionally qualified staff must be conscious of their online image and how it may impact on their professional standing. Even if you do not identify yourself on social media websites by your profession, you must uphold the reputation of your profession at all times. Employees need to be aware that their conduct online can jeopardise their registration and call into question their fitness to practice.

4.4.2 Professionally qualified staff must read and adhere to the social media guidelines produced specifically for their registered bodies e.g., NMC, GMC and HCPC in addition to this protocol. Some of these legislative documents can be sought from the links below:

https://www.nmc.org.uk/globalassets/sitedocuments/nmc-publications/social-media-guidance.pdf – NMC

https://www.gmc-uk.org/ethical-guidance/ethical-guidance-for-doctors/doctors-use-of-social-media/doctors-use-of-social-media#paragraph-8 – GMC

https://www.hcpc-uk.org/registrants/socialmediaguidance/ – HCPC

Please note: this list is not intended to be exhaustive. Employees are responsible for locating the social media guidelines for their own professional bodies.

4.5 Monitoring and Reporting

4.5.1 Any incidents reported either formally or informally to a line manager, including via the raising concerns process, will be reviewed.

4.5.2 Where staff are concerned about any posts or comments made within a social media site, they must print (either manually or provide an electronic print screen copy) of the post and / or comment (showing the time and date) and provide this as evidence when reporting the incident. Line managers who are made aware of an incident must refer to the Standards of Behaviour and Conduct via the Trust's Disciplinary Policy HR03 – Attachment 1 and may wish to seek HR advice if further support is needed.

4.5.3 Breaches in confidentiality or of the Trust's commercial interests must be reported via the Trust's Incident Reporting Procedure OP10 Risk Management and Patient Safety Reporting Policy. The Information Governance Steering Group must be made aware of the breach and will monitor the outcome of the incident.

4.6 Breaches in the Protocol

4.6.1 Any breaches of this protocol bought to the attention of the Trust will be in the first instance be explored and dealt with in accordance with the Trusts Disciplinary Policy (HR03). Breaches to this protocol may constitute gross misconduct, which may result in an employee's dismissal.

4.7 Business Use of Social Media

4.7.1 Using social media is a cost-effective method of connecting with a large, interested audience way beyond the traditional boundaries and catchment area of the large organisation. It offers teams and organisations the opportunity to engage directly with members of the public, partners of the organisation and key stakeholders. It also gives the Trust ability to collect real time feedback and reply to that feedback instantly.

This protocol sets out:

- How the Trust uses social media
- How to obtain a Trust social media account
- What people can or cannot post on the Trust's social media pages and how inappropriate messages are dealt with
- How the Trust's Staff should engage with social networks whilst using Trust social media pages

4.8 The Trust's social media accounts

4.8.1 The Trust engages with its patients, stakeholders, the general public and staff beyond the walls of the hospital by using the corporate website as well as social media. The Trust has the following social media accounts:

Twitter	www.twitter.co.uk/RWT_NHS
Facebook	www.facebook.co.uk/@RWTNHS
Instagram	RWT_NHS
LinkedIn	The Royal Wolverhampton NHS Trust

TikTok RWTNHS

The Trust has also recently launched a closed Facebook group for staff (https://www.facebook.com/groups/weareteamrwt). This is to help us communicate with a wider range of staff and to make our communications more accessible to staff who might not be sitting in front of a computer very often.

Staff are welcome to request to join this group, but it is by no means mandatory.

4.8.2 All of the above accounts are managed by the communications team on behalf of the Trust. They are used as tools to communicate clearly, quickly and in an engaging manner to people interested in the Trust's work.

4.8.3 Staff are advised to use approved messaging systems (for example CareFlo which is certified for use within a Health Care setting) to communicate with teams if it is for business use. The Trust recommends staff do not use messaging systems such as WhatsApp for sharing patient identifiable or Trust sensitive data. Any teams to be found using messaging systems in this way will be the first instance be looked into and dealt with in accordance with the Trusts Disciplinary Policy (HR03).

4.9 Framework

4.9.1 This section describes the broad framework for the setting up, usage, monitoring and management of social media accounts by Trust Staff.

4.9.2 There are many benefits to the Trust in using social media, but to maximise these, and to reduce the risks, it is essential that staff conduct themselves in the correct manner.

4.9.3 Requests for the creation of Trust social media accounts – i.e., those set up by and on behalf of the Trust – must be sent to the Head of Communications who will approve or reject the creation of the accounts.

A social media account will be considered based on the following:

- It is a specialist area that will only appeal to certain people/areas
- The account must be updated frequently and therefore content must be available to upload more than three times a week
- A dedicated individual to be an approved user and go through training with the communications team.

Staff must not establish their own social media forum claiming to be on behalf of the Trust – e.g., the "Information Governance Team at The Royal Wolverhampton Facebook" page is not permitted without appropriate approval (as stated above).

4.9.4 The team which owns and manages the account must work with the Communications Team on the creation and maintenance of the account, and must share the login details with the Communications Team.

4.9.5 When using Trust social media accounts for business use, staff must follow the terms of use set out in this protocol. Failure to do so may result in disciplinary action and could lead to dismissal.

4.9.6 The Trust may choose to communicate with patients, general public and other stakeholders via social media. Only individuals with permission to communicate via social media on behalf of the Trust may use such sites. Permission must be gained by the Head of Communications.

4.9.7 Approved Users

Approved users are Trust staff members who have been granted access to use social media in a professional capacity on behalf of the Trust.

Approved users must:

- Ensure adherence to the terms of the protocol
- Comply with the requirements of any guidance or policies issued by applicable professional bodies including, but not limited to, the Nursing and Midwifery Council, the General Medical Council and the Health and Care Professions Council.
- Obtain consent of any identifiable staff members in images and video before posting this content.
- Not share their personal details, other than their name.
- Not tag individuals in any uploaded images or videos.
- Not show bias towards any specific commercial organisation.
- Not promote or show support for any political party or movement.
- Not use Trust social media accounts to post their personal opinions, or satirise the work of the Trust, its services or wider NHS.
- Provide information in a language other than English if requested. Further information can be sought from the Trust's Patient Advice & Liaison Service (PALS).
- Handle official complaints initially via the Trust's Patient Advice & Liaison Service (PALS).
- Process any freedom of information request in accordance with the Trusts Freedom of Information Policy and Procedure (OP90).
- Process any request relating to Individual Rights (the right to; Access, Rectification, Erasure, Restrict Processing, Data Portability, Objection and in relation to Automated Decision Making) in accordance with the Trusts Health Records Policy (OP07) and the Employee Records Policy (HR09).
- Immediately notify the Communications Team of any query from the press or media.
- Agree to the login details or access for their Trust social media accounts being administered by the Communications Team.
- Not change the account name, login details or access rights for a Trust social media account without the prior agreement of the Head of Communications.
- Upon leaving the Trust, changing role or relinquishing their responsibilities for a Trust social media account, ensure that management of the social media account for which they are responsible is passed to another member of the

team. The previous password can be changed upon request to the Communications Team.

- If no approved colleague is available to assume ownership, transfer ownership of the account to the Communications Team.
- Ensure that any content published:
  - Is consistent with their role in the organisation and with the Trust's vision and values
  - Is relevant and appropriate to the work of the Trust and its services
  - Is not offensive, indecent, obscene or false
  - Does not breach copyright laws
  - Does not compromise the reputation of the Trust or of the NHS
  - Does not breach patient, staff or Trust confidentiality

4.10 Further Information

Any staff who are in doubt about what they should or should not post on social media sites – particularly relating to work of the Trust – or who discover online content that may harm the reputation of the Trust or its services, must speak to their line manager or contact the Communications Team.

The Communications Team regularly monitors content on all Trust social media accounts. If anything is posted onto the accounts that the team thinks is inappropriate, the team will take it down immediately and investigate further. The post may get reinstated following discussion, but this will be the decision of the Head of Communications.

4.11 Breaches in the Protocol

Any breaches of this protocol bought to the attention of the Trust will in the first instance be explored and dealt with in accordance with the Trusts Disciplinary Policy (HR03). Breaches to this protocol may constitute gross misconduct, which may result in an employee's dismissal.

As indicated within section 4 above, professionally qualified staff must read and adhere to the social media guidelines produced specifically for their registered bodies e.g., NMC, GMC and HCPC in addition to this protocol. Some of these legislative documents can be sought from the links below:

https://www.nmc.org.uk/globalassets/sitedocuments/nmc-publications/social-media-guidance.pdf – NMC

https://www.gmc-uk.org/ethical-guidance/ethical-guidance-for-doctors/doctors-use-of-social-media/doctors-use-of-social-media#paragraph-8 – GMC

https://www.hcpc-uk.org/registrants/socialmediaguidance/ – HCPC

Please note: this list is not intended to be exhaustive. Employees are responsible for locating the social media guidelines for their own professional bodies.

5.0 Financial Risk Assessment

1	Does the implementation of this protocol require any additional Capital resources	No
2	Does the implementation of this protocol require additional revenue	No
3	Does the implementation of this protocol require additional manpower	No
4	Does the implementation of this protocol release any manpower costs through a change in practice	No
5	Are there additional staff training costs associated with implementing this protocol which cannot be delivered through current training programmes or allocated training times for staff	No
	Other comments	

6.0 Equality Impact Assessment

An initial equality impact assessment has been carried out and it indicates that there is no likely adverse impact in relation to Personal Protected Characteristics as defined by the Equality Act 2010

7.0 Maintenance

This protocol will be reviewed every three years or earlier if warranted by changing employment needs, amendments to national terms and conditions or employment legislation.

8.0 Communication and training

8.1 All Group Managers, Matrons, Departmental/Directorate Managers are responsible for the communication of this protocol to their staff.

8.2 This protocol can be found on the Trust intranet pages.

8.3 Social media and the provisions surrounding usage will be covered on the Trust's Corporate Induction.

8.4 Advice and guidance can be obtained from the Human Resources Advisory Team and the Communications Team.

8.5 The Communications Team will support approved business users with training on how to use their social media accounts.

9.0 Audit

9.1 The Chief People Officer has overall responsibility for the update and maintenance of this protocol.

9.2 The Divisional Team, as well as the People & Organisational Development Committee will be responsible for monitoring its implementation and reviewing this protocol to ensure it reflects national standards and best practice see below.

Criterion	Lead	Monitoring Method	Frequency	Committee
Personal and Business Use - Fair and consistent use of the protocol	HR Department / Communications Department	Audit of incidents and actions taken by PPC's	Annual	People and Organisational Development Committee
Business use – Checking adherence to protocol	Communications Department	Admin rights to Trust accounts	Annual	People and Organisational Development Committee

10.0 References

British Medical Association – Social Media Guidance for Doctors, July 2017

Data Protection Working Party – Opinion 2/2017 on Data Processing at Work, June 2017

General Medical Council – Doctors' Use of Social Media, April 2013

NHS Digital – Social Media Example Policy, May 2017

NHS Digital – Use of Social Media User Guide, May 2017

NHS Employers – A Social Media Toolkit for the NHS, November 2016

NHS Employers – Using Social Media During Your NHS Career, April 2017

NHS Employers – Facebook Privacy Flyer, April 2017

Nursing and Midwifery Council – Guidance on Using Social Media Responsibly, July 2017

Nursing Times – NMC Guidance: Do's and don'ts for Social Media, July 2011

Attachments
Attachment 1 – Personal Use of Social Media
Attachment 2 – Business Use of Social Media

Appendices
Appendix 1 – How to check your Facebook Privacy Settings in less than 10 minutes

Document Control

<table>
<tr><td>Protocol number and version:
V3</td><td colspan="2">Title
Social Media Protocol</td><td>Status:
FINAL</td><td>Author:
Divisional HR Manager / Head of Communications
Director Sponsor:
Director of Workforce</td></tr>
<tr><td rowspan="4">Version / Amendment History</td><td>Version</td><td>Date</td><td>Author</td><td>Reason</td></tr>
<tr><td>V1</td><td>Jan 2015</td><td>HR Manager</td><td>New</td></tr>
<tr><td>V2</td><td>Oct 2018</td><td>Deputy HR Manager / Head of Communications</td><td>Review & Update of Protocol</td></tr>
<tr><td>V3</td><td>August 2021</td><td>Divisional HR Manager – Advisory/Head of Communications</td><td>Review Date</td></tr>
<tr><td colspan="5">Intended Recipients: All staff, including those working via honorary contracts, secondment contracts, visiting clinical staff, sub-contractors, bank and agency workers, volunteers, apprentices and students working on Trust premises.</td></tr>
<tr><td colspan="5">Consultation Group / Role Titles and Date: Divisional HR representatives, Communication and Staff Side – August 2021</td></tr>
<tr><td colspan="3">Name and date of group where reviewed</td><td colspan="2">Trust Policy Group - December 2021</td></tr>
<tr><td colspan="3">Name and date of final approval committee</td><td colspan="2">Trust Management Committee –
January 2022</td></tr>
<tr><td colspan="3">Date of Protocol issue</td><td colspan="2">February 2022</td></tr>
<tr><td colspan="3">Review Date and Frequency (standard review frequency is 3 yearly unless otherwise indicated)</td><td colspan="2">December 2024 (then every 3 years)</td></tr>
<tr><td colspan="5">Training and Dissemination: Launched via Senior Managers Brief and Divisional Management. Communicated through chairs of approving committees and via the Intranet.
Advice and guidance also available from the HR Advisory Department and The Communication’s Team as and when required by managers and staff.</td></tr>
</table>

To be read in conjunction with:

HR03 – Trust's Disciplinary Policy HR09 – Employee Records Policy

HR06 – Trust's Dispute Resolution in the Workplace Policy

HR16 – Trust's Raising Concerns at Work Policy OP07 – Trust's Health Records Policy

OP10 – Risk Management and Patient Safety Reporting Policy

OP12 – Trust's IT Security Policy

OP13 – Trust's Information Governance Policy GP02 – Local Anti-Fraud, Bribery and Corruption Policy

Equality Impact (Initial) Assessment (all policies): **Completed Yes**

Full Equality Impact assessment (as required): **Completed NA**

If you require this document in an alternative format e.g., larger print please contact the Policy Administrator on ex: 88114

Monitoring arrangements and Committee	People & Organisational Development Committee

Document summary / key issues covered:

This protocol provides guidance to employees on the standards of general conduct and behaviours required for the personal and business use of social media.

The Trust does not wish to deter employees from using social media for personal use, but to highlight where problems can arise.

The protocol highlights the need for employees to protect their privacy when using social media.

The protocol sets out that if staff identify themselves as an employee of the Trust or as an NHS Employee on social media, they must act responsible at all times and uphold the reputation of their profession. Conduct online could still jeopardise employment / registration if it calls fitness to practice into question. Employees are asked to remember to bear in mind that what they may put online as a joke may be misconstrued and could lead to disciplinary action.

Any issue or concern with the Trust must be channelled through the appropriate procedures already in place within the Trust such as the Trust's Dispute Resolution in the Workplace Policy and not displayed or discussed via a social media site. Work-related issues must not be discussed online, including conversations about patients or complaints about colleagues, even when anonymised.

Key words for intranet searching purposes: Social media
Personal use
Business use

High Risk Policy? No

Ratification Assurance Statement

Name of document: Social Media Protocol

Name of author: Louise Sims **Job Title:** Divisional HR Manager - Advisory

I, the above-named author confirm that:

- The Strategy/Policy/Procedure/Guidelines (please delete) presented for ratification meet all legislative, best practice and other guidance issued and known to me at the time of development of the said document.
- I am not aware of any omissions to the said document, and I will bring to the attention of the Executive Director any information which may affect the validity of the document presented as soon as this becomes known.
- The document meets the requirements as outlined in the document entitled Governance of Trust- wide Strategy/Policy/Procedure/Guidelines and Local Procedure and Guidelines (OP01).
- The document meets the requirements of the NHSLA Risk Management Standards to achieve as a minimum level 2 compliance, where applicable.
- I have undertaken appropriate and thorough consultation on this document, and I have detailed the names of those individuals who responded as part of the consultation within the document. I have also fed back to responders to the consultation on the changes made to the document following consultation.
- I will send the document and signed ratification checklist to the Policy Administrator for publication at my earliest opportunity following ratification.
- I will keep this document under review and ensure that it is reviewed prior to the review date.

Signature of Author:

Date:

Name of Person Ratifying this document (Chief Officer or Nominee):

Job Title:

Signature:

- I, the named Chief Officer (or their nominee) am responsible for the overall good governance and management of this document including its timely review and updates and confirming a new author should the current post-holder/author change.

To the person approving this document:

Please ensure this page has been completed correctly, then print, sign and email this page only to: The Policy Administrator.

IMPLEMENTATION PLAN **Procedure/Guidelines number and version** **v.3.0**		**Title of Procedure/Guidelines** **Social Media Protocol**
Reviewing Group	People and Organisational Development Committee	**Date reviewed:** August 2021
Implementation lead: Louise Sims – ADVISORY		
Implementation Issue to be considered (add additional issues where necessary)	**Action Summary**	**Action lead (Timescale for completion)**
Strategy; **Consider** (if appropriate) 1. Development of a pocket guide of strategy aims for staff 2. Include responsibilities of staff in relation to strategy in pocket guide.	Policy will be communicated through the Divisional/ Department Meetings and Trust communication channels.	Upon policy approval HR Advisory Team
Training; Consider 1. Mandatory training approval process 2. Completion of mandatory training form	No training required	n/a
Development of Forms, leaflets etc.; Consider 1. Any forms developed for use and retention within the clinical record **MUST** be approved by Health Records Group prior to roll out. 2. Type, quantity required, where they will be kept / accessed/stored when completed	No additional resources required	n/a
Procedure/Guidelines communication; Consider 1. Key communication messages from the policy / procedure, who to and how?	Launched via management forums, communicated through the chairs of approving committees, via the Intranet and Trust communication channels, and guidance provided by the HR Advisory team.	Upon policy approval HR Advisory Team
Financial cost implementation Consider Business case development	None	
Other specific issues / actions as required e.g., Risks of failure to implement, gaps or barriers to implementation	n/a	

Attachment 1

Personal Use of Social Media

1.1 **Employees must ensure that whilst utilising social media sites, they adhere to high professional standards of behaviour.**

1.2 This protocol sets out the principles for the use of social media **for personal use.** Many people now expect to use social media to interact with each other, and with service providers. The protocol aims to protect employees and prevent them from bringing the Trust and /or wider NHS into disrepute either inadvertently or intentionally.

1.3 This protocol applies to all staff, including those working via honorary contracts, secondment contracts, visiting clinical staff, sub-contractors, bank and agency workers, volunteers, apprentices and students working on Trust premises.

2.0 Use of Social Media at Work for Personal Use

2.1 **Employees must limit their use of social media on Trusts computers or devices to allocated break times only**. Internet use is logged and monitored as per OP12 – IT Security Policy.

2.2 The Trust is aware that employees may wish to bring their own devices such as mobiles and other hand held devices to access social media websites whilst they are at work. **Employees must limit their use of social media on their own equipment to allocated break times only.**

2.3 If an employee states on social media platforms that they work for the Trust, they must be aware of the potential risks associated with this for example members of the public may be able to search for and identify an employee's work location. Adjusting your privacy settings on a social networking site will restrict who can access your profile and will therefore prevent members of the public from finding out personal information about you. Please refer to Appendix 1 – How to check your Facebook Privacy Settings in less than 10 minutes for guidance on how to check your Facebook privacy settings are protected.

2.4 The Trust requires that if an employee chooses to identify that they work for the Trust, on a personal social account they must be aware that members of the public may associate their personal thoughts, actions and behaviours with the Trust and indeed the wider NHS. Stating that, for example 'all my thoughts are my own,' will not safeguard staff against this. Any comments made on social media about colleagues, managers or patients have the potential to be linked to the workplace.

3.0 Personal Use of Social Media

3.1 Whilst using social networking sites for personal use employees must be aware of the image they present online and manage this proactively. The Trust recognises that social media plays a part in everyday life and supports the responsible use by its employees but care needs to be exercised with its use. Used properly, social networking sites such as Facebook are a great way to find old friends, join interest

groups and share information. However, staff must remember that anything posted on a social networking site is in the public domain.

3.2 Staff must recognise that there is a clear relationship between conduct in the real world and conduct online. The Trust has a clear policy on staff rules relating to standards of behaviour and conduct (Trust's Disciplinary Policy HR03 – Attachment 1) and there is an expectation that online conduct must be at a similar high standard.

3.3 Remember everything posted online is public, even with the strictest privacy settings. Once something is online, it can be copied and re-distributed, and it is easy to lose control of it. Presume everything posted online will be permanent and will be shared.

3.4 Staff must recognise that they can bring the Trust into disrepute and damage its reputation.

When using social media staff MUST NOT:

- *Bring the Trust into disrepute* – for example making and/or endorsing defamatory comments about any individuals, organisations, groups, employees or criticising or arguing with service users connected in any way with NHS service provision.
- *Breach confidentiality* – this includes breaching the confidence of patients and staff. Information which could identify patients or service users must not be released: examples include demographic information (name, age and address), diagnosis, ward or area seen (for example ED or outpatients). Confidential information about staff members must also be protected (; this includes information about sickness absence and job roles); unless the staff member has already made the information public knowledge. If you are unsure of whether to publish something, please refer to your line manager or the Trust's Information Governance Policies.
- *Breach the Trust's Commercial Interests* – information about the Trust's business must not be published via social media, this includes information about partner organisations, contracts and internal processes. The Trust will manage the publication of its information through appropriate channels. If you are unsure of whether to publish something, please refer to your line manager or the Trust's Information Governance Policies.
- *Breach Trust Copyright* – by using Trust images or written content without their permission, or by failing to give acknowledgement where permission has been given (unless re-sharing a post that the Trust have made public, i.e. for example re-sharing on Facebook or re-tweeting on Twitter).
- Publish images or make comments that:

- Are considered as bullying, harassment, inflammatory or intimidating in nature.
- Are of a discriminatory, offensive or inappropriate nature. This includes the promotion of discrimination based factors such as race, sex, religion, nationality, disability, sexual orientation or age.
- May create a security risk for the Trust.
- Contain confidential and/or sensitive information; this includes images of Trust information and patients. When posting any images within the

workplace, care must be taken to ensure that no personal identifiable or confidential information is shared. Images of staff members posted onto social media sites must be done with their prior consent.

- Are about patients and/or service users on Social Media. This includes forums such as; WhatsApp groups or Facebook Messenger, even if the forum is private amongst colleagues.
- Are considered slanderous, defamatory, obscene, indecent, lewd, pornographic, violent, abusive, insulting or threatening.
- Use the Internet in any way to attack or abuse colleagues, patients or service users.
- Use social media to promote or assist in any unlawful act.
- Use their NHS email address or contact details to set up their social media or advertise this as a contact address within the social media site.
- Use NHS logos within the site that may give the impressions of official endorsement.
- Use the identity or likeness of another employee, contractor or service user.
- Imply you are authorised to speak on behalf of the Trust.
- Provide professional medical advice through the use of social media.
- Use social media for publicly raising or escalating concerns

This list is not intended to be exhaustive. If there is any doubt about whether a particular activity online is acceptable, it can be useful to think through a real-world analogy. For example, manipulated photos that are intended to mock individuals would be considered offensive if printed and pinned on workplace notice boards, and are no less offensive when shared online, even when privately shared between friends.

3.5 It is not advisable to befriend patients, relatives or carers on social networks, particularly if you use social networks to reveal aspects of your personal life. If a patient contacts you about their care or other professional matters through a personal profile, it is recommended that you indicate that you cannot mix social and professional relationships. In addition to this Trust guidance, professionally registered staff must adhere to any social media guidelines provided by their registering bodies as per section 4.0 of this protocol below.

3.6 Staff must be aware of the consequences of using social media sites to post any content that conflicts with information that they have already provided to the Trust, for example in relation to their health and fitness for work or any secondary employment that they undertake. These actions will bring about possible disciplinary proceedings in line with the Trust's Disciplinary Policy (HR03) and referral to the Trust's Counter Fraud Specialist via the Local Anti-Fraud, Bribery and Corruption Policy (GP02).

4.0 Professional Registration and Social Media

4.1 Professionally qualified staff will put their registration at risk if they fail to adhere to the guidelines above. Professionally qualified staff must be conscious of their online image and how it may impact on their professional standing. Even if you do not

identify yourself on social media websites by your profession, you must uphold the reputation of your profession at all times. Employees need to be aware that their conduct online can jeopardise their registration and call into question their fitness to practice.

4.2 Professionally qualified staff must read and adhere to the social media guidelines produced specifically for their registered bodies e.g. NMC, GMC and HCPC in addition to this protocol. Some of these legislative documents can be sought from the links below:

https://www.nmc.org.uk/globalassets/sitedocuments/nmc-publications/social-media-guidance.pdf – NMC

https://www.gmc-uk.org/ethical-guidance/ethical-guidance-for-doctors/doctors-use-of-social-media/doctors-use-of-social-media#paragraph-8 – GMC

https://www.hcpc-uk.org/registrants/socialmediaguidance/ – HCPC

Please note: this list is not intended to be exhaustive. Employees are responsible for locating the social media guidelines for their own professional bodies.

5.0 Monitoring and Reporting

5.1 Any incidents reported either formally or informally to a line manager, including via the raising concerns process, will be reviewed.

5.2 Where staff are concerned about any posts or comments made within a social media site, they must print (either manually or provide an electronic print screen copy) of the post and / or comment (showing the time and date) and provide this as evidence when reporting the incident.

5.3 Line managers who are made aware of an incident must refer to the Standards of Behaviour and Conduct via the Trust's Disciplinary Policy HR03 – Attachment 1 and may wish to seek HR advice if further support is needed.

5.4 Breaches in confidentiality or of the Trust's commercial interests must be reported via the Trust's Incident Reporting Procedure OP10 Risk Management and Patient Safety Reporting Policy. The Information Governance Steering Group must be made aware of the breach and will monitor the outcome of the incident.

6.0 Breaches in the Protocol

6.1 Any breaches of this protocol bought to the attention of the Trust will be investigated in the first instance and dealt with in accordance with the Trusts Disciplinary Policy (HR03). Breaches to this protocol may constitute gross misconduct, which may result in an employee's dismissal.

Attachment 2

Business Use of Social Media

1.0 Introduction

1.1 Using social media is a cost effective method of connecting with a large, interested audience way beyond the traditional boundaries and catchment area of the large organisation. It offers teams and organisations the opportunity to engage directly with members of the public, partners of the organisation and key stakeholders. It also gives the Trust ability to collect real time feedback and reply to that feedback instantly.

1.2 This protocol sets out:

- How the Trust uses social media
- How to obtain a Trust social media account
- What people can or cannot post on the Trust's social media pages and how inappropriate messages are dealt with
- How the Trust's Staff should engage with social networks whilst using Trust social media pages

2.0 The Trust's social media accounts

2.1 The Trust engages with its patients, stakeholders, the general public and staff beyond the walls of the hospital by using the corporate website as well as social media. The Trust has the following social media accounts:

Twitter	www.twitter.co.uk/RWT_NHS
Facebook	www.facebook.co.uk/@RWTNHS
Instagram	RWT_NHS
LinkedIn	The Royal Wolverhampton NHS Trust

2.2 All of the above accounts are managed by the communications team on behalf of the Trust. They are used as tools to communicate clearly, quickly and in an engaging manner to people interested in the Trust's work.

2.3 Staff are advised to use approved messaging systems (for example CareFlo which is certified for use within a Health Care setting) to communicate with teams if it is for business use. The Trust recommends staff do not use messaging systems such as WhatsApp for sharing patient identifiable or Trust sensitive data. Any teams to be found using messaging systems in this way will be investigated in the first instance and dealt with in accordance with the Trusts Disciplinary Policy (HR03).

3.0 Framework

3.1 This section describes the broad framework for the setting up, usage, monitoring and management of social media accounts by Trust Staff.

3.2 There are many benefits to the Trust in using social media, but to maximise these, and to reduce the risks, it is essential that staff conduct themselves in the correct manner.

3.3 Requests for the creation of Trust social media accounts – i.e. those set up by and on behalf of the Trust – must be sent to the Head of Communications who will approve or reject the creation of the accounts.

3.4 A social media account will be considered based on the following:

- It is a specialist area that will only appeal to certain people/areas
- The account must be updated frequently and therefore content must be available to upload more than three times a week
- A dedicated individual to be an approved user and go through training with the communications team.

3.5 Staff must not establish their own social media forum claiming to be on behalf of the Trust – e.g. the "Information Governance Team at The Royal Wolverhampton Facebook" page is not permitted without appropriate approval (as stated above),

3.6 The team which owns and manages the account must work with the Communications Team on the creation and maintenance of the account, and must share the login details with the Communications Team.

3.7 When using Trust social media accounts for business use, staff must follow the terms of use set out in this protocol. Failure to do so may result in disciplinary action and could lead to dismissal.

3.8 The Trust may choose to communicate with patients, general public and other stakeholders via social media. Only individuals with permission to communicate via social media on behalf of the Trust may use such sites. Permission must be gained by the Head of Communications.

4.0 Approved Users

4.1 Approved users are Trust staff members who have been granted access to use social media in a professional capacity on behalf of the Trust.

4.2 **Approved users must:**

- Ensure adherence to the terms of the protocol
- Comply with the requirements of any guidance or policies issued by applicable professional bodies including, but not limited to, the Nursing and Midwifery Council, the General Medical Council and the Health and Care Professions Council.
- Obtain consent of any identifiable staff members in images and video before posting this content.
- Not share their personal details, other than their name.
- Not tag individuals in any uploaded images or videos.
- Not show bias towards any specific commercial organisation.
- Not promote or show support for any political party or movement.

- Not use Trust social media accounts to post their personal opinions, or satirise the work of the Trust, its services or wider NHS.
- Provide information in a language other than English if requested. Further information can be sought from the Trust's Patient Advice & Liaison Service (PALS).
- Handle official complaints initially via the Trust's Patient Advice & Liaison Service (PALS).

  Process any freedom of information request in accordance with the Trusts Freedom of Information Policy and Procedure (OP90).
- Process any request relating to Individual Rights (the right to; Access, Rectification, Erasure, Restrict Processing, Data Portability, Objection and in relation to Automated Decision Making) in accordance with the Trusts Health Records Policy (OP07).
- Immediately notify the Communications Team of any query from the press or media.
- Agree to the login details or access for their Trust social media accounts being administered by the Communications Team.
- Not change the account name, login details or access rights for a Trust social media account without the prior agreement of the Head of Communications.
- Upon leaving the Trust, changing role or relinquishing their responsibilities for a Trust social media account, ensure that management of the social media account for which they are responsible is passed to another member of the team. The previous password can be changed upon request to the Communications Team.
- If no approved colleague is available to assume ownership, transfer ownership of the account to the Communications Team.
- Ensure that any content published:
  - Is consistent with their role in the organisation and with the Trust's vision and values
  - Is relevant and appropriate to the work of the Trust and it's services
  - Is not offensive, indecent, obscene or false
  - Does not breach copyright laws
  - Does not compromise the reputation of the Trust or of the NHS
  - Does not breach patient, staff or Trust confidentiality

5.0 Further Information

5.1 Any staff who are in doubt about what they should or should not post on social media sites – particularly relating to work of the Trust – or who discover online content that may harm the reputation of the Trust or its services, must speak to their line manager or contact the Communications Team.

5.2 The Communications Team regularly monitors content on all social media accounts. If anything is posted onto the accounts that the team thinks is inappropriate, the team will take it down immediately and investigate further. The post may get reinstated following discussion but this will be the decision of the Head of Communications.

6.0 Breaches in the Protocol

6.1 Any breaches of this protocol bought to the attention of the Trust will be investigated in the first instance and dealt with in accordance with the Trusts Disciplinary Policy (HR03). Breaches to this protocol may constitute gross misconduct, which may result in an employee's dismissal.

6.2 As indicated within section 4 above, professionally qualified staff must read and adhere to the social media guidelines produced specifically for their registered bodies e.g. NMC, GMC and HCPC in addition to this protocol. Some of these legislative documents can be sought from the links below:

https://www.nmc.org.uk/globalassets/sitedocuments/nmc-publications/social-media-guidance.pdf – NMC

https://www.gmc-uk.org/ethical-guidance/ethical-guidance-for-doctors/doctors-use-of-social-media/doctors-use-of-social-media#paragraph-8 – GMC

https://www.hcpc-uk.org/registrants/socialmediaguidance/ – HCPC

Please note: this list is not intended to be exhaustive. Employees are responsible for locating the social media guidelines for their own professional bodies.

HOW TO CHECK YOUR FACEBOOK PRIVACY SETTINGS IN LESS THAN 10 MINUTES

NHS staff can often find themselves part of stories on the news and in the media. To make the stories more relatable, the media use pictures they find online of the people they are reporting on.

Here's what you can do in less than 10 minutes to reduce the likelihood of your holiday snaps on Facebook becoming the ones they use, or worst still, becoming the story.

TOP TIP: The quickest way to access all of the privacy and security settings on Facebook is on a desktop computer.

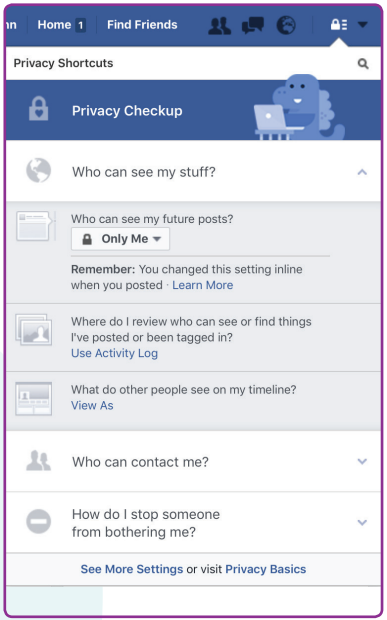
Step 1: Desktop privacy check up (3 mins)

Click the padlock symbol and go through the privacy check up list. Click on the drop down menus under each question to review your current settings.

TOP TIP: Your current and past profile and cover photos are public so make sure these remain professional.

Step 2: View what other people see when they view your timeline and profile (2 mins)

Under the 'Who can see my stuff?' drop down you'll find the very handy 'View as' option. This lets you see how your profile and timeline can be viewed by a member of the public.



Desktop privacy check up screen.

Step 3: Review your photos (5 mins)

You can choose who views the photos you upload to Facebook by selecting which audience sees it. However, if your friend then comments on or shares your photo there is a chance it could be shared with their friends, the public and journalists.

If you uploaded a photo you may choose to delete it. If somebody else uploaded it, click on the 'Allowed on timeline' option under the name of the person who uploaded it and change that to 'Hidden from timeline'. This makes the photo harder to find, but you won't be able to delete it from Facebook yourself as the photo remains the property of the uploader. You could ask the person who posted it to delete it.

TOP TIP:
You can access basic privacy settings from a mobile device, but you cannot access all photo privacy settings from the app.

TOP TIP:
Review and hide any Facebook photo uploads, albums and tagged photos you wouldn't want to become public.

Step 4: Get in the know

Facebook's mission is to make the world more open and connected, therefore it is very hard (if not impossible) to close off your profile, comments, likes and photos from the public. These steps are the basic privacy steps.

Learn more about how Facebook connects content from you and other people together, alongside further privacy settings at **www.facebook.com/about/basics**