University Hospitals Bristol NHS
NHS Foundation Trust

Social Media Policy

Document Data			
Subject:	Social Networking sites		
Document Type:	Policy		
Document Reference	13100		
Document Status:	Approved		
Document Owner:	[redacted]		
Executive Lead:	Director of Workforce and Organisational Development		
Approval Authority:	Trust Partnership Forum		
Review Cycle:	24 Months		
Date Version Effective From:	1/02/2017	**Date Version Effective To:**	1/02/2019

Introduction

This policy is designed to give guidance to all staff on avoiding these risks when using social networking sites.

Document Change Control				
Date of Version	**Version Number**	**Lead for Revisions**	**Type of Revision**	**Description of Revision**
March 2011	V1	Director of Workforce & Organisational Development	Major / Minor	First draft
March 2013	V2	Director of Workforce & Organisational Development	Minor	Revision
January 2015	V3	Director of Workforce & Organisational Development	Minor	Scheduled revision
November 2015	V3.1	Director of Workforce & Organisational Development	Minor	Updated to reflect new Corporate Policy
November 2016	V4	Head of Employee Relations	Minor	Updated to reflect new Corporate Policy

Table of Contents

1. Introduction

University Hospitals Bristol NHS Foundation Trust recognises that the internet is an integral part of the daily lives of staff. Many staff will have access to computer not only within the Trust but at home as well.

The growing popularity of social media sites and applications has raised the risks of staff experiencing potentially serious legal and professional repercussions through the inappropriate use (if only inadvertently) of this recent technology. The facility to access such sites has increased with more staff owning mobile devices such as smart phones or mobile tablets. This trend can affect communications among managers, staff and job applicants, how the Trust promotes and controls its reputation, and how colleagues treat one another.

This policy is designed to give guidance to all staff on avoiding these risks when using social networking sites.

The principles of this policy also apply to the use of Trust e-mail and internal messaging systems.

2. Purpose and Scope

The purpose of this policy is to set guidelines for the use of social media websites and applications ensuring:

- that staff are aware of the potential legal and governance risks associated with the use of social media sites from personal computers/devices;
- that the Trust is not exposed to these legal and governance risks;
- that staff and managers are aware of their responsibilities in relation to social media sites and applications
- that clear and defined procedures are set out to support managers to tackle any use of social media sites and applications which may be in contravention to these guidelines.
- that harassment and bullying by staff via Social Media is eradicated in line with the purpose of the **Tackling bullying and harassment at work policy**

3. Definitions

For the purposes of this policy, social media is a type of interactive online media that allows parties to communicate instantly with each other or to share data in a public forum. This includes online social forums such as Twitter, Facebook and LinkedIn. Social media also covers blogs and videos and image sharing websites such as YouTube and Flickr. This list is not exhaustive and staff should be aware that there are many more examples of social media that can be listed here and this is a constantly changing area. Staff should follow these guidelines in relation to any social media that they use.

This policy applies to all employees of University Hospitals Bristol NHS Foundation Trust. It also applies to agency workers, students, trainees, volunteers and contractors who may not be directly employed by the Trust but are carrying out work on behalf of the Trust. Employees, contractors and agency workers will henceforth be referred to as “staff” for ease.

4. Duties, Roles and Responsibilities

4.1 Divisional Management Boards

Managers should:

- be familiar with this policy and understand when you can view an individual's social media activities (see section 5.5)
- make all of their staff aware of this policy and its provisions
- make staff aware of what cyber-bullying is (see section 5.4)
- directly deal with any contravention of this policy with the member of staff involved in line with the appropriate policy
- seek advice from the Employee Services team if you are unsure how to tackle a particular issue or are not clear about the provisions of the policy
- keep records of all discussions with individual members of staff relating to this policy and its provisions in the form of a file note/record of discussion

4.2 All Staff

All staff should:

- be aware of this policy and comply with the expectations as set out in Section 5, below
- speak to your line manager/supervisor or a member of the Employee Services team if you are not sure about any aspect of this policy.
- speak to your line manager/supervisor or the Employee Services team if you feel they have witnessed behaviour in contravention to the expectations as set out in Section 5.
- be aware of what cyber-bulling is (as defined in section 5.4) and not commit acts of cyber-bulling
- consider whether you want or need your colleagues to see their profile on social media sites and regularly check the privacy settings on your social media pages
- be aware that everything you share on a social networking site could potentially end up in the worldwide public domain and be seen or used by someone you did not intend, even if it appears to be 'private' or is on a closed profile or group

5. Policy Statement and Provisions

5.1 Use of social media at work

Staff must not use social media for their personal use when they are supposed to be working or to the detriment of the expected level of performance

The Trust is aware that phone technology enables staff to access social media sites or other non-work related sites on personal phone applications. Staff must not use their personal phones when they are supposed to be working or to the detriment of the expected level of performance.

Furthermore when staff are working from home using personal computers to undertake Trust business they should not use social media sites or other non-work related sites when they are supposed to be working or to the detriment of the expected level of performance.

The Trust reserves the right to monitor staff usage of social networking sites in work time.

5.2 Use of social media on personal PCs/device

The Trust recognises that a lot of staff may choose to make use of social media in their social lives and in their professional lives and that social media can be a very valuable communications tool in both these arenas. While they are not acting on behalf of the Trust, staff must be aware that they can damage the image of the Trust if they are recognised as being a Trust member of staff, and may bring the Trust into disrepute.

2. When using social media all staff **must** adhere to the following guidelines:

- Avoid any postings or responses on social media which are bullying or harassing in tone towards other members of Trust Staff (this is referred to as Cyber-Bullying see section 5.4)

- Maintain confidentiality of patients and other staff when using social media. Under no circumstances should any patient details or any photographs which may include images of patients be posted via social media.

- Behave professionally, and in a way that is consistent with the Trust's values and policies, if they have identified the Trust as their employer via social media

- When using social networking sites, staff should respect their audience. As a general rule, staff should be mindful of any detrimental comments made about colleagues whilst using social media sites, e.g. failing to show dignity at work (harassment), discriminatory language, personal insults and obscenity. These examples are not exhaustive and will be considered a disciplinary matter.

In addition:

Staff and contractors are ultimately responsible for their own online behaviour. Staff and contractors must take care to avoid online content or actions that are inaccurate, libellous, defamatory, harassing, threatening or may otherwise be illegal. It is possible for staff or contractors to be subject to civil proceedings or criminal prosecution.

Corporate logos or other visible markings or identifications associated with the Trust may only be used where prior permission has been obtained from the communications team.

And all staff **must** not:

- post information about colleagues that they have been asked not to share, and should remove information about a colleague where instructed to do so.
- make disparaging remarks about the Trust, its patients or fellow employees on a social media site
- make any remarks on a social media site that may compromise the Trust.
- air personal grievances related to any aspect of employment with the Trust where others may be able to read them
- post anything which may be considered unlawful or may otherwise bring the Trust into disrepute on their social media site / social media profile page
- take photos or videos on Trust premises and then post these via social media without ensuring there is anything in the photo/video that could breach patient confidentiality, the Data Protection Act or that may bring the Trust into disrepute
- use social media to communicate on behalf of the Trust unless this is a normal accepted part of their role, or through special arrangement that has been approved in advance by the communications team. No social media sites or pages relating to the Trust should be set up by staff and/or contractors without approval, support and advice from the communications team.
- disclose information of the Trust that is or may be sensitive or confidential, or that is subject to a non-disclosure contract or agreement. This applies to information about service users, other staff and contractors, other organisations, commercial suppliers and other information about the Trust and its business activities.
- share details of the Trust's implemented security or risk management arrangements. These details are confidential, may be misused and could lead to a serious breach of security occurring. Staff who may not directly identify themselves as Trust staff members when using social networking sites for personal purpose at home should be aware that the content they post on social media sites could still be construed as relevant to their employment with the Trust.
- unless specifically authorised, post messages under the Trust's name to any newsgroup or chat room

Unauthorised disclosure of confidential information would constitute misconduct /gross misconduct in accordance with the Trust's Disciplinary Policy.

The Trust may also take disciplinary action, if necessary, against any staff member who brings the organisation into disrepute by inappropriate disclosure e.g. comments and photographs on social networking sites or personal internet sites.

Staff should be aware that the Trust reserves the right to use legitimate means to scan the web, including social networking sites for content that it finds inappropriate.

5.3 Professional Networking Sites

The expectation above relating to the avoidance of identification of the Trust on Social Media sites does not apply to professional networking sites, e.g. LinkedIn, where appropriate identification is permitted.

However, all other expectations set out above still apply and contravention will be subject to the same sanctions as set out in Section 5.2 above.

Staff who use social media to interact professionally may state their profession but are encouraged to think carefully about divulging who their employers are within their personal profile pages. If they do state their employer they must behave in a way that is consistent with the Trust's values and policies and should state that they are tweeting/blogging etc. in a personal capacity. Even where staff do not state their employer, they should be aware that they may still be associated with the organisation and the media and others may use what they have posted on their social media accounts if they have access to this.

Professional staff who use social media should ensure that they are aware of the guidance provided by their professional organisations and are encouraged to follow this.

5.4 Cyber Bullying

This section of the policy should be read in conjunction with the Tackling Bullying and Harassment at Work Policy

5.4.1 Definitions

For the purpose of this policy cyber-bullying is defined as:

Bullying, harassment and victimisation conducted through social media such as blogs or social networking.

The Equality Act 2010 defines harassment as:

"unwanted conduct related to a relevant protected characteristic, which has the purpose or effect of violating an individual's dignity or creating an intimidating, hostile, degrading, humiliating or offensive environment for that individual".

The Tackling Bullying & Harassment at Work Policy defines bullying as:

Persistent, unjustified behaviour – either physical or non-physical and often involving a misuse of strength or status – to intimidate, humiliate, harm, or cause loss of confidence to another group or individual.

5.4.2 Further information on cyber-bullying

The Trust has an equal responsibility to prevent staff from being subjected to cyber-bullying, as it does from with alleged bullying, as defined in the Tackling Bullying and Harassment in Work Policy. This includes cyber-bullying that happens outside of work and/or working hours providing the perpetrator works for the Trust and the person affected is either a member of staff, patient, relative, carer or visitor.

Examples of cyber-bullying include:

- posting offensive or threatening comments directed at a member of staff, patient, relative, carer or visitor
- posting inappropriate photographs, or the posting of sensitive personal information of or about a member of staff, patient, relative, carer or visitor
- pressuring staff, patients, relatives, carers or visitors to join online groups

Employees subject to harassment or bullying of any description from any patient, relative, carer or visitor should refer to the Trust "Procedure for the Prevention & Management of Violence and Aggression in the

Workplace". Once made aware of it, the Trust has a legal duty to take reasonable steps to prevent bullying and harassment by people they do not employ.

5.4.3 Victims of cyber-bullying

Staff and managers need to be aware of this type of bullying and that they might be a victim of this behaviour.

If you think you have been a victim of cyber-bullying you should:

- save any evidence of bullying by taking a screen shot of the message- noting the time and date it was sent.
- talk to your line manager or Employee Services (extension 25000, option 3). If your allegation is against your line manager then speak to their manager and consider phoning the Bullying and Harassment Helpline on extension 23406

5.5 The Trust's use of Social Media

5.5.1 Recruiting Managers

Recruiting managers must not, either themselves or through a third party, conduct searches on applicants through social media (apart from appropriate professional networking sites such as Linked in) at any point during the recruitment process. To do so may be seen as discriminatory.

5.5.2 Line Managers

There should be no systematic or routine checking of an individual's online social media activities in line with data protection laws. Significant intrusion into private lives will not normally be justified unless there is a real risk of damage to the Trust. However in exceptional circumstances managers can view an individual's social media account if they suspect serious wrongdoing. Examples of such transgressions include incidents of bullying of colleagues, fraud or social media activity causing serious damage to the Trust. Advice must be sought from Employee Services before taking any action

IM&T can help managers view employee's social media content within work however requests to do this also need to be authorised by Employee Services

6. References

To be read in conjunction with the Guidelines on Social Media Use.

Other relevant Trust documents can be found on Connect on HR Web:

- Disciplinary Policy
- Staff Conduct Policy
- Tackling Bullying and Harassment at Work Policy
- Trust Values
- IG03- Guidance on use of e-mail, internet and electronic office by staff
- Recruitment Policy
- Corporate Social Media Policy

7. Appendix B – Dissemination, Implementation and Training Plan

7.1 The following table sets out the dissemination, implementation and training provisions associated with this Policy.

Plan Elements	Plan Details
The Dissemination Lead is:	[redacted], Interim Head of Employee Relations
This document replaces existing documentation:	Social Media Policy
Existing documentation will be replace by:	No other documentation to be replaced.
This document is to be disseminated to:	All Managers and Employees and will be available on HR Web.
Method of dissemination:	HR Web
Training is required:	Training will be provided for managers by Employee Services on a 121 basis on a case by case basis.
The Training Lead is:	HR Consultants, Employee Services

Additional Comments
n/a

8. Appendix C – Document Checklist

8.1 The checklist set out in the following table confirms the status of 'diligence actions' required of the 'Document Owner' to meet the standards required of University Hospitals Bristol NHS Foundation Trust Procedural Documents. The 'Approval Authority' will refer to this checklist, and the Equality Impact Assessment, when considering the draft Procedural Document for approval. All criteria must be met.

Checklist Subject	Checklist Requirement	Document Owner's Confirmation
Title	The title is clear and unambiguous:	Title is clear
	The document type is correct (i.e. Strategy, Policy, Protocol, Procedure, etc.):	Document type is correct
Content	The document uses the approved template:	Approved template used
	The document contains data protected by any legislation (e.g. 'Personal Data' as defined in the Data Protection Act 2000):	Protected Data.
	All terms used are explained in the 'Definitions' section:	Terms are explained.
	Acronyms are kept to the minimum possible:	Acronyms minimal.
	The 'target group' is clear and unambiguous:	Target group is clear.
	The 'purpose and scope' of the document is clear:	Purpose and Scope are clear.
Document Owner	The 'Document Owner' is identified:	Document Owner is identified.
Consultation	Consultation with stakeholders (including Staff-side) can be evidenced where appropriate:	Consultation is evidenced.
	The following were consulted: Staff Side, Employee Services Team, HR Business Partners.	Consulted
	Suitable 'expert advice' has been sought where necessary:	Suitable advice sought
Evidence Base	References are cited:	References are cited
Trust Objectives	The document relates to the following Strategic or Corporate Objectives:	Trust Objectives.
Equality	The appropriate 'Equality Impact Assessment' or 'Equality Impact Screen' has been conducted for this document:	Equality Impact Assessment completed
Monitoring	Monitoring provisions are defined:	Monitoring provisions are defined.
	There is an audit plan to assess compliance with the provisions set out in this procedural document:	There is an audit plan.

Checklist Subject	Checklist Requirement	Document Owner's Confirmation
	The frequency of reviews, and the next review date are appropriate for this procedural document:	Review frequency and next date are shown
Approval	The correct 'Approval Authority' has been selected for this procedural document:	Approval Authority is appropriate.

Additional Comments
n/a

University Hospitals Bristol NHS Foundation Trust

Guidance on the use of Social Media at work

1. Introduction

University Hospitals Bristol NHS Foundation Trust recognises that the internet is an integral part of the daily lives of staff. Many staff will have access to computer not only within the Trust but on handheld devices and at home as well. This document is a set of guidelines to be read in conjunction with the Corporate Social Media Policy and the Social Media Policy (for Personal use) for further information on appropriate use in a professional setting (see links at the end of this document).

Social Media sites are accessible via trust computers but there are still guidelines we have to work by. These guidelines apply to all employees of University Hospitals Bristol NHS Foundation Trust. It also applies to agency workers, students, trainees, volunteers and contractors who may not be directly employed by the Trust but are carrying out work on behalf of the Trust. Employees, contractors and agency workers will henceforth be referred to as "staff" for ease.

2. Aim

Social media offers great opportunities for the organisation and individuals to listen and communicate in a dynamic and effective way that will benefit our staff and our patients. The next generation of our workforce will never have known a world without social media, the internet and mobile phones. How the Trust embraces this is therefore key to enabling communication with the workforce and beyond to develop and deliver services using the platforms people are most familiar with.

One of the Trust's key priorities is to strengthen staff engagement and communication with staff. Progress on this is monitored annually through the NHS Staff Survey and more frequently via the Staff Friends and Family Test.

Social media enables organisations to connect and engage directly with thousands of people (both staff members and patients) and organisations, be seen to understand and take on board their views and involve them in discussion.

Within the NHS it is estimated that four out of five organisations now use at least one form of social media as part of their official communications and engagement channels. UH Bristol recognises that social media has the potential to reach staff and other stakeholders and is now embracing social media as one of its communication methods.

We Trust our staff with patients' lives so we should be able to trust them with social media. These guidelines aim to guide staff regarding use of Social Media (in conjunction with Trust Policy), to help them get the best out of the tools available whilst maintaining a safe professional environment and protecting themselves, as well as the Trust.

3. Definition of Social Media

Social media is a type of interactive online media that allows parties to communicate instantly with each other or to share data in a public forum. This includes online social forums such as

Twitter, Facebook and LinkedIn. Social media also covers blogs and videos and image sharing websites such as YouTube and Flickr. This list is not exhaustive and staff should be aware that there are many more examples of social media that can be listed here and this is a constantly changing area. Staff should follow these guidelines in relation to any social media that they use.

4. Use of Social Media

When – using social media for personal use should be done in your breaks and not in work time. It should not interfere with working time and everyday tasks.

How - Professional staff that use social media should ensure that they are aware of the guidance provided by their professional organisations and are encouraged to follow this. Staff should not cause offence or needless anxiety to any individual or risk damaging the Trust's reputation. This includes personal use of social media outside of work. Employees should not bring the Trust into disrepute with any information they post on social media.

Volumes – The use of social media should be done in small volumes. Employees are able to use appropriate use of social media websites from trust devices; this should not interfere with the employee's everyday duties. Employees should not spend an excessive amount of time while at work using social media websites.

Communication – Staff must maintain confidentiality of patients and other staff when using social media. Under no circumstances should any patient details or any photographs which may include images of patients be posted via social media.
Staff must also behave professionally, and in a way that is consistent with the Trust's values and policies, if they have identified the Trust as their employer via social media or if they post comments about the Trust.

5. Employees must not:

- Present views on behalf of the Trust, on social media unless you are authorised to do so.
- Use any of the Trust's facilities for commercial activities, this includes running businesses.
- Take part in political activities using the Trust facilities.
- Bring the Trust into disrepute through their use of social media.
- Use their personal devices when they are supposed to be working or to the detriment of the expected level of performance

6. The Trust will:

- Take unauthorised disclosure of confidential information very seriously and this may constitute misconduct /gross misconduct in accordance with the Trust's Disciplinary Policy.
- Take disciplinary action, if necessary, against any staff member who brings the organisation into disrepute by inappropriate disclosure e.g. comments and photographs on social networking sites or personal internet sites.
- Reserve the right to use legitimate means to scan the web, including social networking sites for content that it finds inappropriate.

7. Cyber-bullying

This section should be read in conjunction with the Tackling Bullying and Harassment at Work Policy. Cyber-bullying is defined as:

Bullying, harassment and victimisation conducted through social media such as blogs or social networking.

The Trust has an equal responsibility to prevent staff from being subjected to cyber-bullying, as it does from with alleged bullying, as defined in the Tackling Bullying and Harassment in Work Policy. This includes cyber-bullying that happens outside of work and/or during working hours.

Examples of cyber-bullying include:

- posting offensive or threatening comments directed at a member of staff, patient, relative, carer or visitor
- posting inappropriate photographs, or the posting of sensitive personal information of or about a member of staff, patient, relative, carer or visitor
- pressuring staff, patients, relatives, carers or visitors to join online groups

Employees subject to harassment or bullying of any description from any patient, relative, carer or visitor should refer to the Trust "Procedure for the Prevention & Management of Violence and Aggression in the Workplace". Once made aware of it, the Trust has a legal duty to take reasonable steps to prevent bullying and harassment by people they do not employ.

8. Further Information

If you are unclear of what is appropriate use and need further guidance please see the following Policies:

Corporate Social Media Policy
http://nww.avon.nhs.uk/dms/Download.aspx?did=19124

Social Media Policy (for personal use):
http://nww.avon.nhs.uk/dms/download.aspx?did=13100

Tackling Bullying and Harassment in Work Policy:
http://nww.avon.nhs.uk/dms/download.aspx?did=7839

Guidance on staff use of Email, Internet and the Electronic Office:
http://connect/aboutus/CorporateGovernance/informationgovernance/Lists/DMS%20List/DispForm.aspx?ID=13

Corporate Social Media Policy

Document Data		
Subject:	Trust social media policy	
Document Type:	Policy	
Document Status:	Published	
Document Owner:	Head of Communications	
Executive Lead:	Deputy Chief Executive	
Approval Authority:	Risk Management Group	
Estimated Reading Time:	6 Minutes[1]	
Review Cycle:	36 months	
Next Review Date:	**Date of First Issue:**	**Date Version Effective From:**
[12 January 2018]	[12 January 2016]	[12 January 2016]

Document Abstract

The increasing use of social media is having a growing influence on society. From dictating tomorrow's news today, to giving individuals a public voice, or just helping form new social connections independent of geography, social media has quickly embedded itself within our daily lives.

Social media offers great opportunities for organisations and individuals to listen and have conversations with a wide range of people irrespective of geography. Social media platforms are critical to enabling the NHS to listen and use patients' concerns and ideas to provide a clinically excellent and sustainable NHS.

This policy sets out how University Hospitals Bristol NHS Foundation Trust uses social media to help it achieve its goals and provides guidance for staff and governors on the use of social media.

[1] Divide number of words (1226) by 240 for average reading time and add 25% for specialist content.

Document Change Control				
Date of Version	**Version Number**	**Lead for Revisions**	**Type of Revision**	**Description of Revision**
12/01/2016	1.00	Head of Communications	Major	

Table of Contents

1. Introduction

Social media offers great opportunities for organisations and individuals to listen and have conversations with a wide range of people irrespective of geography, age, mobility and other factors. Social media platforms are critical to enabling the NHS to listen and use patients' concerns and ideas to provide a clinically excellent and sustainable NHS.

University Hospitals Bristol NHS Foundation Trust (UH Bristol) is now making increased use of social media to engage with their patients, service users and other stakeholders, and to deliver key messages for good healthcare and services generally. These online digital interactions are encouraged and their use is likely to be further extended as new communications channels become available.

This policy sets out how University Hospitals Bristol NHS Foundation Trust uses social media to help it achieve its goals and provides guidance for staff and governors about their personal responsibilities for appropriate use of social media. This policy should be read alongside the Social Media (for Personal Use) Policy and Procedure.

This policy is necessary as many employees and contractors enjoy sharing their knowledge and experience with others of similar roles and interests and use of social media is widespread. The Trust encourages these online activities and acknowledges that staff and contractors can improve their personal skills and experience through relevant interactions with others outside the organisation.

However, the Trust has a responsibility to ensure the operational effectiveness of its business, including its public image, reputation and for the protection of its information assets of all kinds. This involves ensuring confidentiality and maintaining security in accordance with NHS Information Governance policy and good practice.

2. Purpose and Scope

The purpose of this policy is to:

- Set out how UH Bristol uses social media to help it achieve its goals;
- Provide clarity to staff on the use of social media tools when acting independently or as a representative of UH Bristol and give them the confidence to engage effectively. (Please note that further guidance for staff on their personal use of social media is contained in the Social Media (for Personal Use) Policy and Procedure.);
- Ensure that the organisation's reputation is not brought into disrepute and that it is not exposed to legal risk; and
- Ensure that internet users are able to distinguish official corporate UH Bristol information from the personal opinion of staff.

The policy applies to all employees, to temporary workers, volunteers, governors, honorary contract holders, students on placement and work experience.

3. Definitions

Social Networking is the term commonly given to websites and online tools which allow users to interact with each other in some way – by sharing information, opinions, knowledge and interests. It involves building online communities or networks, encouraging participation and engagement.

To an individual, social media is anything which allows information to be published, shared and commented on online without the influence of editors or organisations or the state.

To organisations, social media is a selection of online platforms which allow information to be published, shared and commented on online and enable organisations to communicate with individual stakeholders.

4. Duties, Roles and Responsibilities

4.1 Senior Leadership Team (SLT)

(a) As the Senior Leadership Team, SLT is responsible for role modelling appropriate use of social media and ensuring that staff and services within their areas of responsibility are aware of both the potential benefits and pitfalls of social media and approach the communications team for advice and support on the development of social media within their areas.

4.2 Divisional Management Boards

(a) Divisional management boards are responsible for ensuring that services and teams within their divisions are aware of both the potential benefits and pitfalls of social media.

(b) Divisional Management Boards must refer teams or services with a specific communications need for which social media would be helpful to the communications team for advice and support to ensure any social media groups are established using shared learning across the Trust and the appropriate governance frameworks.

4.3 Communications team

(a) The communications team is responsible for maintaining and updating the Trust's social media policy, and for developing and updating the Trust's social media presence via its corporate social media accounts.

(b) The communications team is responsible for providing advice about social media to divisions, departments, and individuals.

(c) The communications team is responsible for providing advice and support to a hospital with specific communication needs for which social media would be helpful. This includes providing guidelines and protocols for how to establish and maintain social media groups, ensuring that information governance is adhered to at all times and that specific accounts or groups are managed using appropriate governance frameworks.

(d) The communications team is responsible for providing advice and support to a team or service with specific communications needs for which social media would be helpful. This includes providing guidelines and protocols for how to establish and maintain social media groups, ensuring that information governance is adhered to at all times and that specific accounts or groups are managed using appropriate governance frameworks.

4.4 All staff and governors

(a) All staff members (as defined in section 3) and governors have a responsibility to abide by this policy.

(b) If a staff member or governor comes across information contained on social media sites that contravenes this policy, they should report the issue through the Trust's incident reporting system Datix. All incidents will be investigated by the relevant department, for example Human Resources, Information Governance or Communications.

4.5 Responsibility for Monitoring Compliance

(a) All incident reports are monitored by the risk management team.

(b) Formal Grievance and Disciplinary matters are monitored by Employee Services and will be reported in a quarterly report to the Trust's Industrial Relations Group.

(c) The communications team reports on its work by exception to the Senior Leadership Team.

5. Policy Statement and Provisions

Staff Use of Social Media

5.1 University Hospitals Bristol NHS Foundation Trust (UH Bristol) is making increased use of social media to engage with their patients, service users and other stakeholders, and to deliver key messages for good healthcare and services generally. It recognises that staff may choose to use social media in their social lives and in their professional lives and that social media can be a very valuable communications tool in both these arenas.

5.2 Staff who use social media to interact professionally may state their profession but are encouraged to think carefully about divulging who their employers are within their personal profile pages. If they do state their employer they must behave in a way that is consistent with the Trust's values and policies and should state that they are tweeting/blogging etc. in a personal capacity. Even where staff do not state their employer, they should be aware that they may still be associated with the organisation and the media and others may use what they have posted on their social media accounts if they have access to this.

5.3 Professional staff who use social media should ensure that they are aware of the guidance provided by their professional organisations and are encouraged to follow this.

5.3 Staff and contractors are not authorised to communicate by any means on behalf of the Trust unless this is an accepted normal part of their job, or through special arrangement that has been approved in advance by the communications team. No social media sites or pages relating to the Trust should be set up by staff and/or contractors without approval, support and advice from the communications team.

5.4 Staff and contractors are ultimately responsible for their own online behaviour. Staff and contractors must take care to avoid online content or actions that are inaccurate, libellous, defamatory, harassing, threatening or may otherwise be illegal. It is possible for staff or contractors to be subject to civil proceedings or criminal prosecution.

5.5 Staff and contractors who use social media must not disclose information of the Trust that is or may be sensitive or confidential, or that is subject to a non-disclosure contract or agreement. This applies to information about service users, other staff and contractors, other organisations, commercial suppliers and other information about the Trust and its business activities.

5.6 Corporate logos or other visible markings or identifications associated with the Trust may only be used where prior permission has been obtained from the communications team.

5.7 Staff and contractors must not share details of the Trust's implemented security or risk management arrangements. These details are confidential, may be misused and could lead to a serious breach of security occurring. Staff who may not directly identify themselves as Trust staff members when using social networking sites for personal purpose at home should be aware that the content they post on social media sites could still be construed as relevant to their employment with the Trust.

5.8 When using social networking sites, staff should respect their audience. As a general rule, staff should be mindful of any detrimental comments made about colleagues whilst using social media sites, e.g. failing to show dignity at work (harassment), discriminatory language, personal insults and obscenity. These examples are not exhaustive and will be considered a disciplinary matter.

5.9 Unauthorised disclosure of confidential information would constitute misconduct /gross misconduct in accordance with the Trust's Disciplinary Policy.

5.10 Staff should be aware that the Trust reserves the right to use legitimate means to scan the web, including social networking sites for content that it finds inappropriate. The Trust also reserves the right to monitor staff usage of social networking sites in work time.

5.11 The Trust may also take disciplinary action, if necessary, against any staff member who brings the organisation into disrepute by inappropriate disclosure e.g. comments and photographs on social networking sites or personal internet sites.

Trust Use of Social Media

5.2 The Trust has a corporate presence on Facebook and Twitter and may develop a corporate presence on other social media channels in the future. These accounts are used to listen and have conversations with a wide range of people irrespective of geography.

5.21 The Trust encourages staff who wish to interact with the Trust, or the Trust's charities, on social media to do so. However, this must be done appropriately, in line with this policy and the Social Media (for Personal Use) Policy and Procedure, considering the Trust's reputation and responsibility for protecting information assets of all kinds. This involves ensuring confidentiality and maintaining security in accordance with NHS Information Governance policy and good practice.

5.22 Hospital-specific social media accounts may be established for one or more of the Trust's hospitals where a specific need for it is identified. Before this goes ahead, a way of working will be established to ensure that the accounts are appropriately used and managed using an appropriate governance framework.

5.23 Some services have specific communications and support needs for their patients. In cases where it is thought these may be provided by social media groups, the Trust's may set up and maintain social media groups specific to groups of patients with specific communication needs. These will be established ensuring the accounts are appropriately used and managed using an appropriate governance framework.

Reporting Inappropriate Behaviour on Social Media

5.3 If a staff member or governor comes across information contained on social media sites that contravenes this policy, they should report the issue through the Trust's incident reporting system Datix.

5.31.2 All incidents will be investigated by the relevant department, for example Human Resources, Information Governance or Communications.

6. Associated Documentation

6.1 UH Bristol's Social Media (for Personal Use) Policy and Procedure.

6.2 The British Medical Association's guide "Using social media: practical and ethical guidance for doctors and medical students"

6.3 The Nursing and Midwifery Council's "Guidance on using social media responsibly".

6.4 NHS Employer's Briefing 87 "HR and social media in the NHS: The essential guide for HR directors and managers".

6.5 UH Bristol's staff conduct policy.

6.6 UH Bristol's IG policy.

7. Appendix A – Dissemination, Implementation and Training Plan

7.1 The following table sets out the dissemination, implementation and training provisions associated with this Policy.

Plan Elements	Plan Details
The Dissemination Lead is:	Head of communications
This document replaces existing documentation:	No existing documentation
Existing documentation will be replace by:	No existing documentation
This document is to be disseminated to:	Divisional directors, clinical chairs, execs, non-execs, governors, heads of nursing, matrons, HR team, all staff via Newsbeat and Connect.
Training is required:	Essential training IG eLearning module
The Training Lead is:	Information Governance Officer

Additional Comments
[DITP - Additional Comments]

8. Appendix C – Document Checklist

8.1 The checklist set out in the following table confirms the status of 'diligence actions' required of the 'Document Owner' to meet the standards required of University Hospitals Bristol NHS Foundation Trust Procedural Documents. The 'Approval Authority' will refer to this checklist, and the Equality Impact Assessment, when considering the draft Procedural Document for approval. All criteria must be met.

Checklist Subject	Checklist Requirement	Document Owner's Confirmation
Title	The title is clear and unambiguous:	Yes
	The document type is correct (i.e. Strategy, Policy, Protocol, Procedure, etc.):	Yes
Content	The document uses the approved template:	Yes
	The document contains data protected by any legislation (e.g. 'Personal Data' as defined in the Data Protection Act 2000):	Yes
	All terms used are explained in the 'Definitions' section:	Yes
	Acronyms are kept to the minimum possible:	Yes
	The 'target group' is clear and unambiguous:	Yes
	The 'purpose and scope' of the document is clear:	Yes
Document Owner	The 'Document Owner' is identified:	Yes
Consultation	Consultation with stakeholders (including Staff-side) can be evidenced where appropriate:	Yes
	The following were consulted:	
	Suitable 'expert advice' has been sought where necessary:	IG officer Trust Secretariat
Evidence Base	References are cited:	Yes
Trust Objectives	The document relates to the following Strategic or Corporate Objectives:	
Equality	The appropriate 'Equality Impact Assessment' or 'Equality Impact Screen' has been conducted for this document:	N/A
Monitoring	Monitoring provisions are defined:	
	There is an audit plan to assess compliance with the provisions set out in this procedural document:	
	The frequency of reviews, and the next review date are	

Checklist Subject	Checklist Requirement	Document Owner's Confirmation
	appropriate for this procedural document:	36 months
Approval	The correct 'Approval Authority' has been selected for this procedural document:	Yes - IRMG

Additional Comments
[DCL - Additional Comments]