Maidstone and Tunbridge Wells NHS Trust

Ref: FOI/GS/ID 5518

Please reply to:
FOI Administrator
Trust Management
Maidstone Hospital
Hermitage Lane
Maidstone
Kent
ME16 9QQ

05 September 2019

Freedom of Information Act 2000

I am writing in response to your request for information made under the Freedom of Information Act 2000 in relation to Staff social media policy.

You asked:
1. Do you have a staff social media policy?
2. Do you have a policy or guidance on staff use of messaging apps, such as WhatsApp, Siilo, Forward?
3. Does your Trust actively discourage the use of WhatsApp?
4. In the past two calendar years, have any staff been formally disciplined for the inappropriate use of messaging apps at work (ie for sharing clinical information) or for using unapproved messaging apps? If yes, how many?
5. Are you aware how many staff use WhatsApp for work-based communication with colleagues? If yes, how many?
6. Have you recommended or implemented a messaging platform for use across your Trust? If yes, which app or platform do you use?

Trust response:

1. Yes. The Trust is currently updating our media policies and the draft update is included below.
2. Please see policies below.
3. Please see policies below

Please see the following current policies and draft addition:

MAIDSTONE AND TUNBRIDGE WELLS NHS TRUST

Social Media Policy and Procedure

Requested/ Required by:	Information Governance Committee
Main author:	Head of Communications, ext 25859
Other contributors:	Department of Health Informatics Directorate
Document lead:	Deputy Chief Executive
Directorate:	Corporate
Specialty:	Trust Management
Supersedes:	Social Media Policy, Procedure and Guidance [Version 1.0: August 2012]
Approved by:	Senior HR Meeting, 14th April 2016
Ratified by:	Policy Ratification Committee, 29th April 2016
Review date:	April 2019

Document history

Requirement for document:	Recommendation – Department of Health • Common Law of Confidentiality • NHS Confidentiality Code of Conduct
Cross references:	• British Medical Association *Using Social Media: Practical and ethical guidance for doctors and medical students* http://bma.org.uk/-/media/Files/PDFs/Practical%20advice%20at%20work/Ethics/socialmediaguidance.pdf • NMC (2015) *The code: standards of conduct, performance and ethics for nurses and midwives* http://www.nmc-uk.org/Nurses-and-midwives/Advice-by-topic/A/Advice/Social-networking-sites/ • RCN Code of Conduct • GMC Code of Conduct • Health Professionals Council Code of Conduct
Associated documents:	• Maidstone and Tunbridge Wells NHS Trust. *IT Acceptable Use Policy* [RWF-OPPCS-NC-TM8] • Maidstone and Tunbridge Wells NHS Trust. *Code of Confidentiality* [RWF-OPPCS-NC-TM3] • Maidstone and Tunbridge Wells NHS Trust. *Anti-Fraud Policy and Procedure* [RWF-OPPPCS-NC-WF48] • Maidstone and Tunbridge Wells NHS Trust. *Disciplinary Policy and Procedure* [RWF-OPPPCS-NC-WF10] • Maidstone and Tunbridge Wells NHS Trust. *Speak Out Safely (SOS) policy and procedure* [RWF-OPPPCS-NC-WF33] • Maidstone and Tunbridge Wells NHS Trust. *Bullying and Harassment Policy and Procedure* [RWF-OPPPCS-NC-WF24]

Version Control:		
Issue:	**Description of changes:**	**Date:**
1.0	Original document	August 2012
2.0	Corrected typing errors, added additional social media profiles, updated Setting up, managing and monitoring Trust social media profiles section	April 2016

Policy statement for

Social Media Policy

Maidstone and Tunbridge Wells NHS Trust (MTW / the Trust) recognises the vital benefits and importance of using social media to communicate and engage with patients, staff and stakeholders, promote the Trust and its services, help raise awareness of public health campaigns and support the Trust's emergency planning role.

This policy is not meant to deter Trust employees from using social media but to help employees understand their responsibilities and prevent them from bringing themselves, the Trust or the NHS into disrepute either inadvertently or intentionally and the potential consequences in doing so.

Staff should be aware of the information risks and good practices associated with the protection of sensitive information in social media and other social interaction scenarios.

Staff are reminded of confidentiality and data protection provisions inherent in contracts of employment. Staff must not disclose confidential information about the Trust or its services whilst using social media. These provisions do not affect staff's entitlement under the Speak Out Safely (SOS) Policy and Procedure (formerly Whistle Blowing).

Social Media Procedure

1.0 Introduction and scope

This policy and procedure applies to all staff, including bank, locum and temporary staff and contractors or agency workers working for, or on behalf of, the Trust.

The policy provides a general awareness of the associated risks of using both personal or MTW corporate social media profiles and how this may potentially affect the effectiveness of Trust services or damage the Trust's reputation.

2.0 Definitions

Social media is the term commonly used for websites that allow people to interact with each other in virtual communities, by sharing information, videos, images, opinions, knowledge and interests. As the name implies, social media involves the building of online communities or networks, encouraging participation and engagement.

Social networking websites (such as Facebook and Twitter*)* are perhaps the most well-known examples of social media, but the term covers other web-based services. Examples include:

- blogs (a contraction of the term web log - a regularly updated website or web page, typically run by an individual or small group, that is written in an informal or conversational style) and vlogs (a contraction of the term video log – a blog in which the postings are primarily in video form)
- audio and video podcasts
- 'wikis' (such as *Wikipedia*)
- message boards (forums)
- social bookmarking websites (such as *del.icio.us*)
- photo, document and video content sharing websites (such as Instagram, Flickr and YouTube)
- micro-blogging services (such as Twitter, Google+, LinkedIn, Facebook*)*
- Mobile messaging services (such as WhatsApp and video messaging application Snapchat

Blagging: the term commonly used to describe the deliberate, reckless and potentially criminal obtaining and/or disclosing of personal information about individuals without that person's knowledge or valid consent.

Trojan: a Trojan horse, or Trojan, is malware that appears to perform a desirable function for the user prior to run or install but instead facilitates unauthorized access of the user's computer system. *"It is a harmful piece of software that looks legitimate. Users are typically tricked into loading and executing it on their systems"*, as Cisco describes.

Malware: short for *malicious software*, is software designed to secretly access a computer system without the owner's informed consent. The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code.

Phishing: is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication. Communications purporting to be from popular social web sites, auction sites, online payment processors or IT administrators are commonly used to lure the unsuspecting public. Phishing is typically carried out by email or instant messaging, and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Phishing is an example of social engineering techniques used to fool users, and exploits the poor usability of current web security technologies. Attempts to deal with the growing number of reported phishing incidents include legislation, user training, public awareness, and technical security measures.

Instant messaging (**IM**): is a form of real-time direct text-based communication between two or more people using personal computers or other devices, along with shared software clients. The user's text is conveyed over a network, such as the Internet. More advanced instant messaging software clients also allow enhanced modes of communication, such as live voice or video calling.

3.0 Duties (roles and responsibilities)

Staff should remember that all individuals are bound by the Common Law of Confidentiality and the NHS Confidentiality Code of Conduct. Failure to comply with this policy whilst blogging or using social media sites may result in disciplinary action being taken by the Trust that could, ultimately, depending on the seriousness of any breach, result in dismissal.

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

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

Employees should be mindful of the Trust's policies and procedures and Codes of Conduct that are part of their employment and professional requirements. These include:

- The confidentiality clauses in contracts of employment;
- The Trust's Disciplinary Policy and Procedure and Bullying and Harassment Policy and Procedure;
- Professional Codes of Conduct (e.g. Nursing and Midwifery Council, General Medical Council, Health Professions Council and the Royal College of Nursing).

Any breach of any of the above may be deemed gross misconduct and may result in disciplinary action being taken. Employees' actions may also have

legal implications. They may be committing actionable defamation or breach of confidentiality. The latter could also have professional consequences.

Staff are also legally liable if they breach legislation relating to the gathering, storage or processing of data at all times. Therefore, everyone who manages or handles personal information within MTW must:

- understand that they are contractually responsible for following good data protection practice;
- be aware of their responsibilities and obligations to respect confidentiality
- be appropriately trained to do so; and
- be appropriately supervised

3.1 Communications Team

The Communications Team lead on all social media activity for the Trust, managing, updating and monitoring the Trust's corporate social media profiles and social media activity.

The Communications Team also help Directorates set up service social media accounts, train staff in managing and monitoring those profiles and provide basic reputation management, and tone and brand awareness training. In addition, they oversee the management of service-led social media profiles.

Through their role as social media lead, the Communications Team may, from time to time, identify comments or posts on social media from employees, which could potentially be inappropriate. In these circumstances the Communications Team will forward any relevant posts and associated information to the local / Directorate manager, and if appropriate HR, for them to follow up.

3.2 Managers

Where it has been identified a member of staff has potentially posted inappropriately, their line manager will handle any follow-up locally, and if relevant, seek advice from HR with regards to relevant HR policies.

3.3 Human Resources (HR)

HR will guide and advise local managers on HR matters in relation to any potentially inappropriate social media activity by a member of staff.

3.4 Information Governance

Information Governance provides a central point of information for all data protection matters. Information Governance provides training on the gathering, storage and processing of data to all staff.

4.0 Training / competency requirements

It is mandatory for all staff, including new starters, locum, temporary, students and contract staff members, to complete, on an annual basis, information governance training. The principles of confidentiality are covered in this training.

Staff wishing to set up and manage a corporate social on behalf of the Trust must receive training from the Communications Team.

5.0 The risks of social media and mitigations

5.1 Why are blogging and social networking an Information Governance issue?

The use of blogging and social networking websites by employees can expose the organisation to information risks, even where these sites are not accessed directly from work.

5.2 What are the potential dangers to the organisation of using blogging and social networking?

5.2.1 Unauthorised disclosure of business information and potential confidentiality breach

Blogging and social networking sites provide an easy means for information to leak from an organisation, either maliciously or otherwise. Once posted to a site, organisational information enters the public domain and may be processed and stored anywhere globally. In short, organisational control is lost and reputational damage can occur.

5.2.2 Malicious attack associated with identity theft

People often place a large amount of personal information on social networking sites, including details about their nationality, ethnic origin, religion, addresses, date of birth, telephone contact numbers and interests. This information may be of use to criminals who are seeking to steal identities or who may use the information for social engineering purposes.

5.2.3 Legal liabilities from defamatory postings by employees

When a user registers with a site they typically have to indicate their acceptance of the site's terms and conditions. These can be several pages long and contain difficult to read legal language. Such terms and conditions may give the site 'ownership' and 'third party disclosure' rights over content placed on the site, and could create possible liabilities for the Trust. For example, where a user is registering on a site from a PC within the Trust, it may be assumed that the user is acting on behalf of the Trust and any libellous or derogatory comments may result in legal action. In addition, information being hosted by the website may be subject to other legal jurisdiction overseas and may be very difficult to correct or remove.

5.2.4 Reputational damage

Ill-considered or unjustified comments or images left on sites may adversely affect public opinion toward an individual or the Trust. This can lead to a change in social or business status with a danger of consequential impact.

5.2.5 Malicious code targeting social networking users causing virus infections and consequential damage

Sites may encourage or require the download and installation of additional code in order to maximise the site's functionality and potential value. Where sites have weak or ineffective security controls

it may be possible for code to be changed to contain malicious content such as viruses and Trojans, or to trigger unintended actions such as phishing.

5.2.6 Systems overload from heavy use of sites with implications of degraded services and non-productive activities

Sites can pose threats to the Trust's information infrastructure. Particularly as the use of rich media (such as video and audio) becomes the norm in such sites, the bandwidth consumption generated by these sites can be significant and they have the potential to be the biggest bandwidth consumers within an organisation.

5.3 How has the Trust responded to these risks?

Whilst technical controls have been applied to block or control undesirable website usage the main defence against threats associated with using social media is user awareness.

Knowledge of the potential problems related to blogging and social networking will help employees in their safe use of such services and help protect the Trust.

5.4 Advice to help avoid problems when using social media

Appendix 4 aims to help employees use social media whilst maintaining a safe professional environment and protecting themselves and the Trust.

On registration, understand what you are signing up to and importantly what security and confidentially claims and undertakings exist. Watch for add-ons i.e. additional features or applications that change the terms and conditions of what you have signed up for, or that may require changes to the security settings of your devices.

Examine carefully any email coming from social networking sites or contacts as these may be unreliable containing malicious code or be spoofed to look as though they are authentic.

Please refer to Appendix 4 for a guide to the dos and don'ts on using social media.

5.5 Acceptable / inappropriate use

The Trust has a reasonable and lawful expectation that staff will not bring the Trust into disrepute. This is extended to the home environment as well.

Any grievance with the organisation or an individual who is employed directly by the Trust should be channelled through procedures and policies already in place and dealt with within the work environment.

If staff become aware of a breach in this policy, they have a duty to contact their line manager in the first instance, if it is appropriate to do so. It is possible such a matter may be resolved locally, although HR would act to support line managers if this was not the case and further action needed to be taken.

Work devices

Employees may access social networking sites, not blocked by the Trust, for personal purposes but should not do so during the working day. Staff should be mindful of the Trust Anti-Fraud Policy and Procedure in relation to using such sites for their own personal use, particularly in respect to abuse of Trust assets and property.

5.6 Personal devices

Employees accessing social media sites on their personal devices should not do so during working time.

Additional guidance for registered healthcare professionals

In addition to popular social networking sites such as Facebook and Twitter, there are a number of well-established sites aimed specifically at medical professionals, such as doctors, nurses, physiotherapists, medical students and occupational therapists.

Practical and ethical guidance is available from:

- British Medical Association (BMA) - http://bma.org.uk/-/media/Files/PDFs/Practical%20advice%20at%20work/Ethics/socialmediaguidance.pdf
- Nursing and Midwifery Council (NMC) – http://www.nmc-uk.org/Nurses-and-midwives/Advice-by-topic/A/Advice/Social-networking-sites/
- Health and Care Professions Council - http://www.hcpc-uk.org/Assets/documents/100035B7Social_media_guidance.pdf

Setting up, managing and posting to Trust corporate social media profiles

The Communications Team sets up, manages and runs all corporate Trust social media profiles.

The Communications Team is responsible for updating the main Trust profiles, which are:

Twitter: www.twitter.com/mtwnhs
Facebook: www.facebook.com/mymtwhealthcare
LinkedIN: www.linkedin.com/company/maidstone-and-tunbridge-wells-nhs-trust
NHS Choices:
www.nhs.uk/Services/Trusts/Overview/DefaultView.aspx?id=1178

The Communications Team also sets up Trust social media profiles for services and helps manage these alongside staff from that department. Examples of these profiles include:
www.facebook.com/pages/The_Wells_Suite
www.facebook.com/mtwmaternity
www.facebook.com/mtwchildrens
www.facebook.com/mtwpatientresearchambassador
www.twitter.com/mtwhealthphys

If your service or department is interested in managing a social media profile on behalf of the Trust, you must contact the Communications Team in the first

instance. Under no circumstances should staff set up a corporate profile without prior approval from the Communications Team, or having received training from the Communications Team.

Information posted to Trust service or department social media profiles must have a corporate, professional tone and be relevant to patients, stakeholders and visitors using that service or department.

If you are aware of any Trust service or department that use social media, and they are not one of those listed above, please report these to the Communications Team.

You can contact the Communications Team at: mtw-tr.communications@nhs.net

01622 228658

Good practice tips to recognise and address potential problems associated with blagging

1. Be suspicious of all unsolicited contacts including phone calls, visits, faxed messages, email, SMS messages asking for information about other staff, contractors and patients.
2. Ensure you take steps to verify the identity of the caller/sender.
3. Do not provide information about the Trust, patients or other individuals unless you are certain of the recipient's identity and authority to have the information requested.
4. Avoid disclosing personal or other sensitive information.
5. Don't send personal or other sensitive information over the Internet unless you are completely confident in the website's legitimacy and implemented security.
6. If you think you have been a victim of blagging ensure you immediately report this as an incident, in the first instance, to your line manager.

6.0 Monitoring and audit

This policy will be reviewed following ad-hoc incidents throughout the year.

APPENDIX ONE

Process requirements

1.0 Implementation and awareness

Communication plan

This policy needs to be communicated to all staff, this will be achieved by:

- Once ratified the PRC Chairman will email this policy/procedural document to the Clinical Governance Assistant (CGA) who will activate it on the Trust approved document management database on the intranet, under 'Policies & Q-Pulse'. Q-Pulse
- A monthly publications table is produced by the CGA which is published on the Trust intranet under 'Policies & Q-Pulse'; notification of the posting is included on the intranet "News Feed" and in the Chief Executive's newsletter.
- On reading of the news feed notification all managers should ensure that their staff members are aware of the new publications.
- Global communication and supporting documentation
- Making paper copies available
- Informing staff of the policy during Induction and IG training sessions

2.0 Review

The policy will be reviewed every three years. If substantive changes are required to the policy during this time it will be resubmitted to the review group.

3.0 Archiving

The Trust approved document management database retains all superseded files in an archive directory in order to maintain document history. Documents submitted as part of the Trust Information Governance Toolkit and similar audit returns will be retained for a minimum of three years.

APPENDIX TWO

CONSULTATION ON: Social Media Policy and Procedure

Please return comments to: Head of Communications

By date: 1 April 2016

Name:	Date sent	Date reply received	Modification suggested? Y/N	Modification made? Y/N
Local Counter Fraud Specialist	18/03/16			
Senior Information Risk Owner (SIRO)	18/03/16			
Caldicott Guardian	18/03/16			
Director of Health Informatics	18/03/16			
Information Asset Owners	18/03/16	18/03/16	Y	Y
Head of Legal Services	18/03/16			
Director of Human Resources	18/03/16	18/03/16	Y	Y
Head of Information Governance	18/03/16			
HR committee	18/03/16	19/04/16	Y	Y
Head of Emergency Planning & Response	06/07/16			
The role of those staff being consulted upon as above is to ensure that they have shared the policy for comments with all staff within their sphere of responsibility who would be able to contribute to the development of the policy.				

APPENDIX THREE

Equality Impact Assessment

In line with race, disability and gender equalities legislation, public bodies like MTW are required to assess and consult on how their policies and practices affect different groups, and to monitor any possible negative impact on equality. The completion of the following Equality Impact Assessment grid is therefore mandatory and should be undertaken as part of the policy development and approval process. **Please note that completion is mandatory for all policy development exercises. A copy of each Equality Impact Assessment must also be placed on the Trust's intranet.**

Title of Policy or Practice	Social Media Policy and procedure
What are the aims of the policy or practice?	To ensure all staff are aware of the responsibilities in respect to data protection
Identify the data and research used to assist the analysis and assessment	
Analyse and assess the likely impact on equality or potential discrimination with each of the following groups.	**Is there an adverse impact or potential discrimination (yes/no).**
Males or Females	No
People of different ages	No
People of different ethnic groups	No
People of different religious beliefs	No
People who do not speak english as a first language	No
People who have a physical disability	No
People who have a mental disability	No
Women who are pregnant or on maternity leave	No
Single parent families	No
People with different sexual orientations	No
People with different work patterns (part time, full time, job share, short term contractors, employed, unemployed)	No
People in deprived areas and people from different socio-economic groups	No
Asylum seekers and refugees	No
Prisoners and people confined to closed institutions, community offenders	No
Carers	No
If you identified potential discrimination is it minimal and justifiable and therefore does not require a stage 2 assessment?	
When will you monitor and review	At the time of review of the

your EqIA?	policy/procedure
Where do you plan to publish the results of your Equality Impact Assessment?	As Appendix Three of this policy/procedure on the Trust approved document management database

FURTHER APPENDICES

The following appendices are published as related links to the main policy /procedure on the Trust approved document management database:

No.	Title	Unique ID
4	Dos and don’ts regarding social media	RWF-OPG-CORP44

ICT Acceptable Use Policy and Procedure (AUP)

This document sets out the Trust Acceptable Use Policy for ICT systems

Requested/ Required by:	Information Governance Steering Committee
Main author:	Director of ICT
Other contributors:	n/a
Document lead:	Director of ICT **Contact Details:** ext. 22048
Directorate:	Corporate
Specialty:	Trust Management
Supersedes:	ICT Acceptable Use Policy (Version 1.0: October 2004)
Approved by:	Information Governance Committee, 13 March 2013
Ratified by:	Trust Executive Committee, 20th March 2013
Review date:	March 2014 *Director of Health Informatics as Chair of the Information Governance Committee has approved an extension to the review date until **December 2017**

Document history

Document name	MTW ICT AUP.docx
Version	2.0
Date issued	14/03/2013
Document location	Q:\Information Governance\ICT Master Documents\
Document asset no.	TBC

Requirement for document	This policy is required to meet NHS Information Governance and IM&T data security requirements.
Cross references:	Compliance with national information Governance requirements and NHS assurance standards. Legislation: • Data Protection Act 1998 www.informationcommissioner.gov.uk www.opsi.gov.uk • Computer Misuse Act 1990 www.opsi.gov.uk • Regulatory Investigation Powers Act (RIPA) • Copyright, Designs and Patents Act 1998 www.opsi.gov.uk • Health and Safety at Work Act www.opsi.gov.uk • Human Rights Act 1998 www.opsi.gov.uk
Associated documents:	• Maidstone and Tunbridge Wells NHS Trust. *Information Security Policy* [RWF-OPPCS-NC-TM11] • Maidstone and Tunbridge Wells NHS Trust. *Email Policy and Procedure* [[RWF-OPPCS-NC-TM6]

Version control

Version	Comment	Date
1.0	Original policy	October 2004
2.0	New AUP replaces IT Acceptable Use Policy v1.0 (October 2004)	13/03/2013
2.1	Director of Health Informatics as Chair of the Information Governance Committee has approved an extension to the review date until December 2017	June 2017

Policy Statement for

ICT Acceptable Use Policy

As a user of IT services of the Trust you have a right to use its computing services; that right places responsibilities on you as a user which are outlined in this policy. If you misuse Trust computing facilities in a way that constitutes a breach or disregard of the following policy, consequences associate with that breach and you may be subject to disciplinary procedures.

Ignorance of this policy (or those that it directs you to), and the responsibilities it places on you, is not an excuse in any situation where it is assessed that you have breached the policy and its requirements.

A specific policy governing the use of email by staff is available on the Trust document management system and should be read in conjunction with this IT Acceptable Use Policy.

For the purposes of this policy the term "***computing services***" refers to any IT resource made available to you, any of the network borne services, applications or software products that you are provided access to and the network/data transport infrastructure that you use to access any of the services (including access to the Internet).

ICT Acceptable Use Procedure

Contents

1.0 Introduction and scope

The information technology (IT) facilities at the Maidstone and Tunbridge Wells NHS Trust are provided to support the operation of the hospital, teaching, learning and research.

Set out below is a Code of Practice regarding the use and security of the organisation's IT facilities.

The Code of Practice provides a framework for operating within a rapidly evolving area of activity. It may appear to be restrictive but it is actually meant, in spirit, to be a means of enabling all users to obtain maximum benefit from the available IT facilities.

The term 'users' which appears throughout the Code of Practice includes all employees, students, volunteers and contractors and other users of Trust provided PCs connected to the Trust network via dial-in facilities and any others who may be authorised to use the IT facilities.

This document should be read as an overall statement of acceptance of the information management policies of the Trust; specifically, but not limited to the: Information Security Policy.

1.1 Overall principles

All users are required to comply with the Trust ICT Acceptable Use Policy.

Failure to comply with the Acceptable Use Policy will lead to the suspension of your use of the IT facilities whilst the circumstances are investigated. A serious failure to comply with the Policy is a disciplinary issue within the organisation.

The penalties for failing to comply will range in severity from loss of access to facilities, to suspension or dismissal from the organisation. Some forms of computing equipment misuse are a criminal offence; such misuse will be referred to the Police.

1.2 General conditions

- Your use of the Trust's computing services must at all times comply with the law.
- Your use of the Trust's computing services must not interfere with any others' use of these facilities and services.
- You are not entitled to use a computer that you have not been authorised to use.
- You must not access any program or data which has not been specifically authorised for your use.
- You must not use or copy any data or program belonging to other users without their express and specific permission.
- You must not alter computer material belonging to another user without the user's permission.
- You must not use Trust computing services to harass, defame, libel, slander, intimidate, impersonate or otherwise abuse another person.

- You must not use Trust computing services for the creation, collection, storage, downloading or displaying of any offensive, obscene, indecent or menacing images, data or material capable of being resolved into such. (There may be certain legitimate exceptions for Trust purposes which would require the fullest disclosure and special authorisations)
- You must not use the Trust's computing services to conduct any form of commercial activity without express permission.
- You must not use the Trust's computing services to disseminate mass (unsolicited) mailings.
- You must not install, use or distribute software for which you do not have a licence.
- In general, use of Trust "computing services" should be for the provision of healthcare, research, teaching or the administrative purposes of the Trust. Modest use of the facilities and services for personal use is accepted so long as such activity does not contravene the conditions of this policy.
- Use of "computing services" for commercial work may be governed by software licence constraints and users should verify that the intended use is permissible under the terms of those licences with the IT Support Staff or with the Kent & Medway Health Informatics Service.

2.0 Definitions

Users: includes all employees, students, volunteers, contractors and other users of Trust provided PCs connected to the Trust network via dial-in facilities and any others who may be authorised to use the IT facilities.

3.0 Duties

Key duties are outlined within the body of the procedure (Sections 5.0 – 16.0).

4.0 Training / competency requirements

No training / competency requirements are defined at present.

5.0 General provisions

The use of IT systems for personal purposes is permitted provided that it does not interfere with the user's operational effectiveness (i.e. it is within legitimate break periods). The Trust reserves the right to monitor the use of IT systems, which may include the examination of individual usage, to safeguard against abuse.

The Trust also reserves the right to grant a manager, subject to authorisation by the appropriate Head of Department, access to a user's mailbox in instances where the user is unavailable, for whatever reason, to meet operational needs. Where such access is provided, the reason for the access will be documented.

The user will be notified that mailbox has been opened and the purpose for which the mailbox was accessed.

The following list is provided as a guide and staff should be made aware of any local arrangements in their department. Access to staff email may be granted where the information required:

- Directly relates to service users, staff, service or operational matters.
- Information is required urgently.
- Information is related to urgent staff, operational or departmental information, report and/or data which cannot be obtained by any other means.
- Is not for personal or private interest.
- An examination of the email is required as part of an investigation.

The use of IT systems for illegal or criminal purposes is strictly prohibited.

Any user who finds a possible security lapse on any IT system is obliged to report it to the IT Department. You should not attempt to use the system under these conditions until the problem has been investigated.

All users should be aware that periodic security checks are conducted on IT systems, including password checks. Users may be required to change their passwords on request.

Other than as indicated above, electronic mail on all IT systems is private. Attempts to read another person's electronic mail or other protected files will be treated with the utmost seriousness.

IT systems could be adversely affected by an unnecessary large scale use of system resources (e.g. inappropriate use of disk space, download time, printer time etc.) The deliberate wasting of network resources or of the time of staff involved in the support of such systems will lead to the withdrawal of access to these facilities.

The creation, transmission or reception (other than for properly supervised and lawful research purposes) of any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material is strictly prohibited.

The creation or transmission of material which is designed or likely to cause annoyance, inconvenience or needless anxiety to others, including chain letters, obscene or nuisance messages, sexist or racist messages of any form or defamatory material is strictly prohibited.

Use of facilities by outside individuals or organisations requires special permission from the IT department and the possible payment of license fees.

Use of IT facilities for commercial uses, except by approved license holding organisations, is strictly prohibited.

IT facilities must not be used for the transmission of unsolicited commercial or advertising material either to other user organisations on the NHS network or to other user organisations on other networks.

Personal data must not under any circumstances be stored on Trust equipment, local and network drives and Trust issued storage devices.

Personal data found on Trust drives will be deleted without notice to the owner.

Users should avoid wherever possible sending email attachments on internal mail, particularly to large groups. Wherever possible users should provide a

link in the body of the email to a single copy of the document located on a shared drive or intranet site.

6.0 Security and privacy of user accounts

Each individual user is responsible for all matters concerning the proper use of their account. All users **must** ensure that they:

- **Choose** safe passwords.
- **Do not** share passwords with another person.
- **Do not** share their account with another person.
- **Do not** make unauthorised attempts to gain access to any account belonging to another person.
- **Do not** attempt to gain access to any IT systems to which they should not have access.
- **Do not** attempt to gain unauthorised access to other systems.
- **Do not** create material that infringes the copyright of another person.
- **Do not** send e-mails to users who do not need to see them.

Deliberate activities with any of the following characteristics are strictly prohibited:

- Corrupting or destroying other users' data.
- Violating the privacy of other users (other than those activities undertaken in connection with usage monitoring as specified in above)
- Disrupting the work of other users.

7.0 Intellectual property

The Trust recognises that respect for intellectual property and individual creativity is vital to academic discourse and enterprise. This applies to works of all authors and publishers in all media. It encompasses respect for the right to acknowledgment, the right to privacy, and the right to determine the form, manner and terms of publication and distribution.

As electronic information is volatile and easily reproduced, respect for the work and personal expression of others is especially critical in computer environments. Violations of authorial integrity, including plagiarism, invasion of privacy, unauthorised access, and trade secrets and copyright violations, may be grounds for sanctions against users.

The codes of practice and regulations of the organisation provide a framework with respect to intellectual property rights with which all users are required to comply.

8.0 Internet access

Internet access is via NHSnet which is monitored for inappropriate use. The use of the Internet in a way which could lead to action being taken against the Trust by the NHSnet Security Board will be treated as a serious disciplinary offence.

Internet sites often offer an opportunity to download material. If this happens - be careful. If the Internet site is not instantly recognisable as a reputable site, e.g. a government department or public company then exercise caution. Consult the IT department in any case where the provenance of the material to be downloaded cannot be guaranteed.

Occasionally you may receive a message which tells you that, in order to receive a download; you must first load a piece of enabling software. If this happens, contact the IT department. Do not download software yourself onto the Trust network.

Games software which has been copied or downloaded, screen savers which have been downloaded and email attachments are recognised as prime sources of computer viruses (see section 12 below). Users are required to assume that all downloadable games, screen savers and email attachments, as well as games software which has been copied to a disk, are capable of carrying viruses.

The downloading of games and screen savers or any other installation of such software by IT users is strictly prohibited.

The Trust assumes no liability for personal financial transactions carried out across the Internet e.g. purchase of goods from online shopping sites.

9.0 Electronic mail

a) Only specific email addresses are considered secure. Users should never send Strictly Private or Confidential messages by email unless prior consent has been obtained from the addressee or unless approved encryption, i.e. an acceptable method of ensuring privacy and authenticity, is used. Always assume that email is not secure unless you have ensured that it is being sent via secure through encryption. If in doubt consult the Trust's Email Policy or ask the IT Department.

b) Email sent externally must only go out via NHSmail to another NHSmail account or similarly secure email account, those ending:

GSI	*.gsi.gov.uk
CJX	*.police.uk or .pnn.police.uk
GSE	*.gse.gov.uk
GSX	*.gsx.gov.uk
GCSX	*.gcsx.gov.uk
SCN	*.scn.gov.uk
CJSM	*.cjsm.net - the branding for the CJIT system
MoD	*.mod.uk

c) Do not send any patient confidential information to any e-mail address, including your own personal e-mail address, where the address is outside of NHSmail without using encryption and password protection. Do not send more confidential information than is necessary for clinical purposes.

d) You must always use the Bcc function in your email when sending to multiple recipients.

e) Avoid inadvertently entering into any contractual commitments through the use of email.

f) Do not infringe the copyright of others by downloading, copying or transmitting their work to third parties. If you wish to use material produced by another, make sure that you have their permission first.

g) Do not import non-text files or messages onto IT facilities without first having scanned them for viruses.

h) Contact the IT Department if you become aware of a virus.

i) Do not create network congestion through email by sending trivial messages or unnecessarily copying or forwarding email e.g. chain letters or humorous stories.

10.0 General guidance

a) The speed at which email communications can be produced and sent can affect the amount of thought and reflection that would normally be given to the content of a message.

b) Check your email to ensure that the content is appropriate.

c) Be clear and concise in what you say in email messages. Improper statements can give rise to personal or business liability and can be requested for disclosure under the Data Protection Act 1998 or Freedom of Information Act 2000.

d) Email messages that have been deleted may still exist on back-up media or in other storage areas.

e) Do not send information concerning bank accounts or credit cards in email communications.

f) Check your mailbox for messages at regular intervals. You should also make appropriate arrangements for your mail to be forwarded or accessed by others during periods of planned or unplanned absence from the organisation.

g) Make copies of email, saved into an appropriate network folder, which needs to be kept for record keeping purposes.

h) It is the user's personal responsibility to manage retention of emails. Emails should be treated in the same way as other forms of correspondence and it is for the user to determine whether or not an email should be retained. The national NHS Email system does not provide an archive facility so deleted emails may not be easy to recover.

i) Mailboxes will normally be cleared within a few months of a user leaving the Trust. It is the manager's responsibility to ensure that all information that may be required at any future date is transferred to a suitable alternative location.

11.0 Using External Web 2.0 Services

Web 2.0 services offer attractive and useful applications services (Blogs, wikis, office systems, social bookmarking and social networking) to mention but a few. Use of such services however must comply with this policy. Before

using such services – or expecting others to do so – it would be sensible to appreciate the issues that pertain to them.

Pros

- They may offer ready access to the latest, flexible technology.
- The social aspects of many services are enhanced by very widespread usage – there is no point in the Trust attempting to replicate del.icio.us or Facebook.
- Registration, account creation and access is normally very quick and cheap if not free.
- They offer routes to research collaboration or to peer group interaction.

Cons

- It is easy to be tempted to produce, and submit, content to such sites that you might later regret.
- What content or comments you do submit becomes potentially available across the world.
- Such content may have a longer life span than you might have imagined and could be accessed by a wide audience, including potential employers.
- Although such sites are external to the Trust, the way in which you use them, or the content that you submit to them might still lead you into trouble with the Trust and its policies and regulations.

Always read and consider the terms and conditions for any service you register with and ensure that you understand the implications of the service conditions.

Be aware that such services may be hosted overseas and as such you are required to ensure that you are able to comply with the 8th principle of the Data Protection Act 1998 - Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

12.0 Viruses

A computer virus is a piece of software which has been written by someone with the specific intention of disrupting the normal operation of a computer or network. Computer viruses are usually written in such a way that they are capable of spreading from one computer to another and from one network to another.

Viruses can seriously affect the 'health' of a computer and by so doing they have the potential to severely affect any work which users are trying to do on a computer or network which has been 'infected' by a virus.

Viruses may have varying effect on computers and networks. At one extreme the only effect may be that a mischievous message appears on a screen once and is never seen again, there may be an intermittent malfunction of a computer or, at the other extreme, there may be a complete loss of all data and systems files on a computer or network. A computer or network may be out of action for a significant period of time following the introduction of a

virus. The consequent loss of work stored on such a computer can be devastating to the user.

Viruses are most commonly introduced to a computer system by either downloading software or documents which contain a virus from a source on the Internet or by inserting external storage media (e.g. A USB memory stick) which already has a virus.

13.0 Trust equipment

Staff must not allow family or friends to use Trust owned equipment.

14.0 Breaches of this policy

Incidents which are determined to be in contravention of this policy will be assessed for their severity. Investigating such incidents may require the collection and evaluation of user related activity and evidence.

It is not possible to provide an exhaustive list of potential ways in which a user may contravene this policy but in general such breaches will be categorised into one of three levels of severity and each level of breach will carry with it a possible range of sanctions, consequences and/or penalties.

Minor breach

This level of breach will attract a verbal warning which will be held recorded for 12 months. In general this category will relate to behaviour or misuse of computer facilities that can be characterised as disruptive or a nuisance. Examples of this level of non compliance would include:

- Taking food and/or drink into IT facilities where they are forbidden.
- Playing computer games on Trust provided IT
- Sending nuisance (non-offensive) email
- Behaving in a disruptive manner.

Not all first offences will automatically be categorised at this level since some may be of a significance or impact that elevates them to one of the higher levels of severity.

Moderate breach

This level of breach will attract more substantial sanctions and/or penalties. These include:

- The Senior Information Risk Owner will be informed of the nature and consequence of the offence.
- Access to computing facilities and services may be withdrawn (account suspension).

Examples of this level of non-compliance would include:

- Repeated minor breaches within the above detailed 12 month period.
- Unauthorised access through the use of another user's credentials (username and password) or using a computer in an unauthorised area.
- Assisting or encouraging unauthorised access.
- Sending abusive, harassing, offensive or intimidating email.
- Maligning, defaming, slandering or libeling another person.

- Misuse of software or software licence infringement.
- Copyright infringement.
- Interference with workstation or computer configuration.

Severe breach

This level of breach will attract more stringent sanctions, penalties and consequences than those above, and access to computing facilities and services may be withdrawn (account suspension) until the disciplinary process and its outcomes have been concluded. Possible sanctions include:

- Notification to the Senior Information Risk Owner
- Withdrawal of access to computing facilities and services.
- For the most serious cases, referral via the SIRO under the formal disciplinary procedures.

Examples of this level of breach would include:

- Repeated moderate breaches.
- Theft, vandalism or willful damage of/to IT facilities, services and resources.
- Forging email, i.e. masquerading as another person.
- Loading, viewing, storing or distributing pornographic or other offensive material.
- Unauthorised copying, storage or distribution of software.
- Any action, whilst using Trust computing services and facilities deemed likely to bring the Trust into disrepute.
- Attempting unauthorised access to a remote system.
- Attempting to jeopardise, damage circumvent or destroy IT systems security at either the Trust or at any other healthcare provision site.
- Attempting to modify, damage or destroy another authorised users data
- Disruption of network communication capability or integrity through denial of service attacks, port scanning, monitoring, packet spoofing or network flooding activities.

14.2 Breach investigation process

An investigation will be carried out, in confidence, under the direction of the Director of Health Informatics. For staff, that investigative report will be passed to the member of staff's Clinical Director or Head of Corporate Directorate, to be considered within the Trust's disciplinary procedures. If a verbal warning is appropriate, this will be given by the Director of Health Informatics. If the breach is more serious, the report will be passed to the Director of Strategy and Workforce to be considered under the Trust disciplinary procedures. Each step of disciplinary procedures provide for an appeal stage.

15.0 Further information

For more information on Trust policy and procedures for the management of information please see the Information Governance leaflets published on the Trust Intranet.

16.0 Monitoring and audit

Activities regarding network transactions may be monitored and logged and kept for an appropriate amount of time. Logs are taken for reasons of security, diagnostic and account/audit reasons. Logs are available only to authorised systems personnel and kept for no longer than necessary and in line with current data protection guidelines.

Such records and information are sometimes required - under law - by external agencies and authorities. The Trust will comply with such requests when formally submitted.

APPENDIX ONE

Process requirements

1.0 Implementation and awareness

- Once approved the document lead/author will send this policy/procedural document to the Clinical Governance Assistant who will publish it on the Trust approved document management database.
- A monthly table of Trust publications will be produced by the Clinical Governance Assistant; this will be published on the Bulletin Board (Trust intranet) under “Trust Publications”, and a notification email circulated Trust wide by the COMMS team.
- On receipt of the Trust wide Bulletin Board notification all managers should ensure that their staff members are aware of the new publications.

2.0 Review

This policy / procedure will be reviewed annually or sooner if changes in legislation or Trust practice require.

3.0 Archiving

The Trust approved document management database retains all superseded files in an archive directory in order to maintain document history.

APPENDIX TWO

CONSULTATION ON: ICT Acceptable Use Policy and Procedure

Consultation process – Use this form to ensure your consultation has been adequate for the purpose.

Please return comments to: *Head of Information Governance*

By date: 5 March 2013

Name: *List staff to be included in the consultation. See Section 5.5 of the "Production, Approval and Implementation of Policies and Procedures" policy and procedure for guidance.*	**Date sent dd/mm/yy**	**Date reply received**	**Modification suggested? Y/N**	**Modification made? Y/N**
Local Counter Fraud Specialist	22-2-13			
Director of ICT	22-2-13			
SIRO	22-2-13			
Caldicott Guardian	22-2-13			
Director of Corporate Affairs	22-2-13			
Director of Strategy and Workforce	22-2-13			
Head of Information	22-2-13			
Head of Health Records	22-2-13			
Staff Side Representative	22-2-13			
Local Security Management Specialist	22-2-13			
Directorate Clinical Directors	22-2-13			
Matrons	22-2-13			
Workforce Business Partners	22-2-13			
Head of Quality and Governance	22-2-13			
Trust Risk Manager	22-2-13			
Clinical Governance Assistant	30-1-13	07-2-13	Y	Y
The role of those staff being consulted upon as above is to ensure that they have shared the policy for comments with all staff within their sphere of responsibility who would be able to contribute to the development of the policy.				

APPENDIX THREE

Equality Impact Assessment

In line with race, disability and gender equalities legislation, public bodies like MTW are required to assess and consult on how their policies and practices affect different groups, and to monitor any possible negative impact on equality.

The completion of the following Equality Impact Assessment grid is therefore mandatory and should be undertaken as part of the policy development and approval process. Please consult the Equality and Human Rights Policy on the Trust intranet, for details on how to complete the grid.

Please note that completion is mandatory for all policy development exercises. A copy of each Equality Impact Assessment must also be placed on the Trust's intranet.

Title of Policy or Practice	ICT Acceptable Use Policy and Procedure
What are the aims of the policy or practice?	To ensure users of the Trust ICT systems are aware of their responsibilities
Identify the data and research used to assist the analysis and assessment	
Analyse and assess the likely impact on equality or potential discrimination with each of the following groups.	**Is there an adverse impact or potential discrimination (yes/no). If yes give details.**
Males or Females	No
People of different ages	No
People of different ethnic groups	No
People of different religious beliefs	No
People who do not speak English as a first language	No
People who have a physical disability	No
People who have a mental disability	No
Women who are pregnant or on maternity leave	No
Single parent families	No
People with different sexual orientations	No
People with different work patterns (part time, full time, job share, short term contractors, employed, unemployed)	No
People in deprived areas and people from different socio-economic groups	No
Asylum seekers and refugees	No
Prisoners and people confined to closed institutions, community offenders	No

Carers	No
If you identified potential discrimination is it minimal and justifiable and therefore does not require a stage 2 assessment?	
When will you monitor and review your EqIA?	Alongside this policy/procedure when it is reviewed.
Where do you plan to publish the results of your Equality Impact Assessment?	As Appendix Three of this policy/procedure on the Trust approved document management database.

Draft wording for update to policies:

Use of Stand Alone Instant Messaging (IM)
It is recognised that IM can be useful in supporting the delivery of direct care. The Trust has reviewed various guidance documents, issued by NHS Digital in recent months, and it has been agreed the use of these tools will be permitted, on a controlled basis, as there are important data protection matters that must be considered, met and/or mitigated.

Data Protection Considerations
Encryption –

- Only Apps and Tools which are able to meet the NHS end-to-end encryption standard of AES 256 bit will be considered for use.
- Data must be encrypted whilst in transit and whilst at rest.

Access Controls –

- Only Apps and Tools which require end-user verification via a minimum two phase authentication will be considered for use.
- Services such as Amazon Web Services or Microsoft Azure must be configured to ensure that the data contained therein is not accessible to unauthorised users.
- Apps and Tools which permit self-registration will only be authorised for use in exceptional circumstances.

Data Storage –

- The Apps and Tools being used should store data within the UK, European Economic Area, a country deemed adequate by the European Commission or in the US where covered by Privacy Shield and must meet the requirements of ISO 27001 or equivalent.
- Apps and Tools that facilitate ‘Remote-wipe’ if a device is lost, stolen or redeployed to another staff member will be considered above those Apps and Tools that do not.

Records Management – Instant Messaging
The amount of person identifiable data communicated via IM should be kept to the minimum possible.

Any clinical decisions or advice received relating to patient care should be transcribed and attributed to the relevant Healthcare Record as soon as possible.
All IM communications may be subject to freedom of information or subject access requests.

Preferred Solutions – Instant Messaging

Hospify
Telegram
WhatsApp (for non-patient data or in the event of a major incident)

3. We allow our staff to use WhatsApp within the Trust guidelines. Please see the response to Q5.
4. In the past two calendar years there has been no formal disciplinary cases which relate to the inappropriate use of messaging apps at work.
5. The Trust employs over 5000 staff who are permitted to use WhatsApp within the Trust guidelines. Please see the following all staff communication:

<u>Use of WhatsApp or other instant messaging applications</u>

Consideration has been given this week to the use of instant messaging communication tools. In response to the recent media coverage on the use of WhatsApp a spokesman for NHS England said 'whatever the other merits of WhatsApp, it should never be used for the sending of information in the professional healthcare environment'. The rationale for this response is that messages can too easily be sent to the wrong contacts, people can pick up unlocked devices – or even bypass passwords. That said, WhatsApp proved very useful during the recent Terrorist incidents in Manchester and London and the Grenfell Tower incident, enabling various agencies to co-ordinate activities and share logistical information. It has therefore been agreed that WhatsApp may be used in the event of emergencies such as a major incident to help call in staff and update staff but limited to non-patient specific information.
Guidance issued December 2017
6. Please see the above draft wording for update to policies.