Maidstone and Tunbridge Wells
NHS Trust

Ref: FOI/GS/ID 4361

Please reply to:
FOI Administrator
Trust Management
Maidstone Hospital
Hermitage Lane
Maidstone
Kent
ME16 9QQ
Email: mtw-tr.foiadmin@nhs.net

21 February 2018

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 Health Apps.

1) Does your trust have a policy on the use of health apps?
2) If yes, please provide the policy (or policies) and contact details.
3) Do you currently have specific budgets for the use of health apps within your trust?
4) If yes, please provide a contact for any budgets related to the use of health apps.
5) Are there individual health apps specified for patient use? Please provide a list of these.
6) If yes, please specify which of these health apps is paid for by the trust.
7) Please specify who is responsible for the funding of each app that is paid for by the trust and provide contact details?

1) No this is covered under the IT acceptable user policy.
2) Policy can be found below.
3) No. This would come out of the overall IT capital budget or local departmental revenue budgets.
4) Not applicable.
5) None currently.
6) Not applicable.
7) Not applicable.

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**

Disclaimer: Printed copies of this document may not be the most recent version.
The master copy is held on Q-Pulse Document Management System
This copy – REV2.1

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.