### Mobile Device Policy

**Version 5**

<table>
<thead>
<tr>
<th>Type of Document</th>
<th>Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Code</td>
<td></td>
</tr>
<tr>
<td>Policy Sponsor</td>
<td>Deputy Director of Informatics</td>
</tr>
<tr>
<td>Lead Executive</td>
<td>Director of Informatics</td>
</tr>
<tr>
<td>Recommended by</td>
<td>Health Informatics Managers</td>
</tr>
<tr>
<td>Date Recommended</td>
<td>12.03.2013</td>
</tr>
<tr>
<td>Approved by</td>
<td>IG Steering Group</td>
</tr>
<tr>
<td>Date Approved</td>
<td>15.05.2013</td>
</tr>
<tr>
<td>Author (s)</td>
<td>Director – ICT, Network Manager</td>
</tr>
<tr>
<td>Date Issued</td>
<td>May 2013</td>
</tr>
<tr>
<td>Review date</td>
<td>May 2015</td>
</tr>
<tr>
<td>Target Audience</td>
<td>Trust staff and patients</td>
</tr>
<tr>
<td>Document Purpose</td>
<td>Define acceptable use of trust issued mobile devices and use of personal devices on trust premises and/or to access Trust services</td>
</tr>
<tr>
<td>Training Requirements</td>
<td>None</td>
</tr>
</tbody>
</table>
| Associated Documents and Key references | Information Security Policy  
Information & Governance Policy  
Confidentiality code of conduct  
H&S policies (Pat testing Chargers)  
Acceptable Use Policy  
Password Policy  
Asset management policy |
| Key Words        | ipad, blackberry, tablet, phone, slate, mobile, vpn, remote, BYOD, IM |
Consultation, Communication

<table>
<thead>
<tr>
<th>Consultation Required</th>
<th>Authorised by</th>
<th>Date Authorised</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analysis of the effects on equality</td>
<td>Not Applicable</td>
<td></td>
<td></td>
</tr>
<tr>
<td>External stakeholders</td>
<td>Not Applicable</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trust staff consultation via intranet</td>
<td>Start date: None</td>
<td></td>
<td>End date:</td>
</tr>
</tbody>
</table>

Implementation Plan

Describe the implementation plan for the policy (and guidelines if impacts upon policy) (Considerations include: launch event, awareness sessions, communication/training via divisions and other management structures etc)

Policy will be uploaded to Intranet; a paragraph raising awareness will be entered in team brief. When new mobile devices are issued the recipient will be made aware they must read the policy and sign the acceptance form.

<table>
<thead>
<tr>
<th>Timeframe for implementation?</th>
<th>RAG</th>
<th>Who is responsible for delivery?</th>
</tr>
</thead>
<tbody>
<tr>
<td>October 2012</td>
<td></td>
<td>Network Manager</td>
</tr>
</tbody>
</table>

Performance Management of Policy KPI's (expected outcomes)

Describe Key Performance Indicators (KPIs) expected outcomes

<table>
<thead>
<tr>
<th>How will the KPI be monitored?</th>
<th>Which committee will monitor this KPI?</th>
<th>Frequency of review?</th>
<th>Lead</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trust Complaints</td>
<td>IG Steering Group</td>
<td>Monthly</td>
<td>IG Steering Group Chair Person</td>
</tr>
</tbody>
</table>

Current version is held on the policy section of the intranet
Performance Management of minimum NHSLA process for this policy

Learning from experience

<table>
<thead>
<tr>
<th>Minimum requirement to be monitored</th>
<th>Process for monitoring e.g. audit</th>
<th>Responsible individual/group/committee</th>
<th>Frequency of monitoring</th>
<th>Performance management of minimum requirements. Responsible individual / group / committee (plus frequency of review / timescales) for:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Audits</td>
<td>HIS Network Manager</td>
<td>Quarterly</td>
<td>Review of results</td>
</tr>
<tr>
<td>Only Approved devices are accessing Network</td>
<td></td>
<td></td>
<td></td>
<td>Monitoring of action plan and implementation</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Development and update of action plan</td>
</tr>
</tbody>
</table>

Who is responsible for producing action plans if deficits in KPI’s and associated processes identified

<table>
<thead>
<tr>
<th>HIS Network Manager</th>
<th>HIS Management Team Meeting</th>
<th>Quarterly</th>
</tr>
</thead>
</table>

How does learning occur?

<table>
<thead>
<tr>
<th>Monitoring of daily processes. Information obtained will be disseminated through HIS team meetings and reinforced with changes to SOPs where appropriate</th>
<th>IT Operations Manager</th>
<th>Annually</th>
</tr>
</thead>
</table>

Current version is held on the policy section of the intranet
## Document Version History

<table>
<thead>
<tr>
<th>Date</th>
<th>Author Designation</th>
<th>Summary of Key changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>September 2012</td>
<td>Assistant Director - ICT</td>
<td>This document combines the Mobile Device Policy with the Mobile Phone Policy and adds sections related to use of personal devices to access Trust services such as e-mail.</td>
</tr>
<tr>
<td>February 2013</td>
<td>Assistant Director – ICT &amp; Network Manager</td>
<td>Policy reviewed to incorporate changes to encompass the Bring Your Own Device project</td>
</tr>
</tbody>
</table>

Current version is held on the policy section of the intranet
CONTENTS

Policy Aim........................................................................................................ p6
1. Introduction............................................................................................... p6
2. Policy Objectives........................................................................................ p6
4. Definitions ................................................................................................ p6
5. Duties Accountabilities and Responsibilities ............................................. p7
6. Processes ................................................................................................ p8
7. Equality Analysis ...................................................................................... p15
8. Training ................................................................................................ p17

Appendices:

APPENDIX A: ACCEPTANCE FORM
APPENDIX B: BOYD TERMS AND CONDITIONS
APPENDIX C: BYOD LOAN MOBILE PHONE AGREEMENT

Current version is held on the policy section of the intranet
EXECUTIVE SUMMARY

Policy Aim

This policy aims to enable staff to utilise the benefits of mobile devices including personally owned devices whilst maintaining the confidentiality and integrity of Trust data. In addition, the policy provides guidance to staff re acceptable use of mobile devices by patients and visitors. This policy sets out the criteria for issue of Trust provided mobile devices and devices that utilize the BYOD Service, the rules around their use, use of personal devices by staff, and acceptable use of Mobile devices on Trust premises by patients/visitors.

1. INTRODUCTION

The Trust is committed to achieving maximum benefit from mobile technology whilst maintaining the necessary environment to ensure patient confidentiality and safety. This policy sets out the Trust’s criteria for issue of mobile devices, the rules around their use, use of personal devices by staff, and acceptable use of Mobile devices on Trust premises by patients/visitors.

2. POLICY OBJECTIVES

- Define the criteria for Trust issued mobile phones and computing devices
- Define the rules for use of personal BYOD devices on Trust premises and with Trust systems
- Facilitate utilisation of new mobile computing innovations
- Define the related services offered by the HIS
- Keep the trust’s data secure
- Define acceptable for patients and visitors
- Identify individual and team responsibilities in achieving these objectives

3. DEFINITIONS

A mobile device in this context is any mobile phone, smartphone, pager, any portable computer e.g. laptop, tablet, iPad, Ipaq, PDA or camera.

The COIN (community of interest network) is the computer network link which connects all the computing resources in STHK and the locality supported by STHK HIS together.

VPN (virtual private network) allows users to connect to the STHK COIN securely over the internet.

BYOD (Bring Your Own Device) refers to the use of personal mobile devices to access NHS Services through the Trust network.

Current version is held on the policy section of the intranet
IM (Instant Messaging) allows a user to connect with a colleague for a quick response to a question using an application that runs on a mobile device or PC.

This policy relates to use of both Trust supplied and privately owned mobile devices and is applicable to all employees, including permanent or temporary staff, contract staff, students, patients and visitors to the Trust.

4. DUTIES, ACCOUNTABILITIES AND RESPONSIBILITIES

St Helens & Knowsley Health Informatics Service (HIS) is responsible for

- Publishing the policy and maintaining a list of permitted mobile devices on the Trust Intranet and notifying staff of any updates or changes.

- Ensuring any investigations of alleged abuse of use as described in this policy are properly conducted by line management (escalating as appropriate) and that any consideration of disciplinary action is instigated in accordance with the Trust’s disciplinary procedures.

- The maintenance of an asset register of all Trust supplied mobile devices and of personal devices allowed to connect to the Trust email system and other services.

- A loan phone will be made available to any Trust employee that meet the following criteria for a seven days, should their own device become lost damaged or stolen -
  - They have surrendered their Trust provided mobile phone and is using their own personal device in its place
  - They are using their own personal device as a business tool

Management Responsibilities

It is the responsibility of Service Managers, Heads of Departments and other budget holders to:

- Formally authorise mobile device requests.

- Identify funding from within their budget to finance mobile device(s) for member(s) of their staff.

- Recover mobile devices from staff leaving the organisation and notify STHK HIS promptly. Line managers will be responsible for making sure that this has been done as part of the normal handing back of Trust property.

- Trust Management reserves the right to refuse to issue a mobile device or to recall a device from any member of staff at its discretion.

- Take full responsibility for a Loan mobile phone signed for by their member of Staff if that device becomes lost, stolen or damaged beyond economical repair.

Current version is held on the policy section of the intranet
Staff Responsibilities

- To sign for receipt of the mobile device, and to acknowledge that they have read, understood and will comply with the requirements of this policy.

- To take good care of the mobile device and take all reasonable precautions to ensure that the device is not damaged, lost or stolen. In the event that your Trust issued device is stolen, staff will be expected to raise an Incident Report, report the theft to the police and obtain an incident number.

- If you lose either a Trust issued device, or a personal device connected to Trust systems, you must inform Informatics via the IT Helpdesk immediately so it can be disabled and where possible wiped remotely. Your device must be secured in a case at all times.

- Staff with a personal BYOD device that becomes lost, damaged or stolen will be entitled to a loan phone for a period of 7 Days whilst they source a replacement. This can be arranged by contacting the IT Helpdesk. The recipient must sign for the loan phone.

- Staff using a Trust issued mobile device or personal mobile device must ensure that the device has a sufficiently charged battery to last a working shift.

- Staff leaving the Trust must return their Trust provided mobile device to their line manager.

- Staff members leaving the Trust that have been connected to the BYOD service must inform the IT Helpdesk so that their device can be removed from the system.

- The Informatics Service will perform a system cleanup on BYOD devices not seen on the Network for a 3 month period. Any such devices will be removed from the system.

Trust staff must:
- Comply with this Policy at all times whilst on Trust business
- Be aware of the patient and visitor guidelines on acceptable mobile device usage
- Report any incidents such as inappropriate use or security breaches to their line manager
- Action will be taken as a result of non-compliance with this policy in line with the Trust disciplinary procedure.

5. PROCESS

5.1 Qualifying Criteria for Business Supplied Mobile Devices
Mobile devices will be provided to those staff whose duties require them to be contactable/on-line when away from their normal place of work.
Sometimes a duty will be covered by issuing a shared mobile device.

In all cases approval to issue a device must be given by the line manager.

Examples of need are (note: this list is not exhaustive):

- Duties require working across multiple sites
- There is a genuine need to be easily and immediately contactable during and outside of normal working hours
- Staff who work in several locations within the hospital
- Staff contractually required to be on call

This policy applies to all members of staff of the St Helens & Knowsley Teaching Hospitals NHS Trust wishing to apply for a mobile device for business use or to transfer an existing mobile device from another organisation

### 5.2 Mobile Devices in Acute Trust Buildings

The use of mobile devices within Acute Trust buildings is permitted for staff, patients and visitors but usage is subject to these guidelines:

The Medicines and Healthcare products Regulatory Agency (MHRA) has said that in certain circumstances the electromagnetic interference from mobile phones can interfere with some medical devices, particularly if used within 2 metres of such devices – DH publication “Using mobile phones in NHS hospitals” January 2009

Mobile devices should not be used within 2 metres of medical devices.

Patient confidentiality must be respected – do not discuss patient details loudly in public areas.

You must show consideration for others by not causing a disturbance when using a mobile device.

Patients and visitors can obtain guidance on acceptable use of mobile devices within St Helens & Knowsley NHS Acute Trust buildings from the St Helens & Knowsley NHS Acute Trust Internet web site by using the URL below:

*Insert URL here once guidelines are published on the Internet site*

Staff can also access the patient and visitor guidelines from the St Helens & Knowsley NHS Acute Trust Intranet web site by using the URL below:

*Insert URL here once guidelines are published on the Intranet site*

Page 9 of 23
Mobile Device Policy, Version 5 -May 2013

Current version is held on the policy section of the intranet
5.3 Mobile Devices and Driving

The Trust's policy on the use of mobile devices while driving is guided, first and foremost, by a concern for the well-being of our staff and other road users. Driving whilst using a mobile device is distracting and can lead to accidents; you cannot be in full control of your vehicle if you are using a hand-held mobile device while driving.

The law says drivers must have proper control of their vehicles at all times and you can be prosecuted for careless or inconsiderate driving, or even dangerous driving, if using a mobile device causes you to drive in this way. The penalties include an unlimited fine, disqualification and up to two years imprisonment. From December 1 2003, it is an offence to drive whilst using a hand-held mobile device with offenders liable to an "on the spot" £60 fine and three points, rising to a maximum of £1,000 if the case goes to court.

Whilst on Trust business you must never use a hand-held device while driving. It is recommended that whenever possible you keep the device switched off or on silent. Only use the device after you have stopped in a safe place.

The Trust recommends that it is best not to use a hands-free device while driving; using a hands-free device while driving will still distract you.

Although you may think that a hands-free device will enable you to control the vehicle, your mind will not be fully on your driving. It is not like talking to a passenger who is aware of the traffic conditions and can see what is happening while you are driving.

5.4 Use of Cameras

The use of cameras in hospital is restricted to respect patient confidentiality, privacy and dignity. Cameras, including camera facilities on mobile devices, are not allowed in secluded areas such as toilets, bathrooms and treatment rooms. A member of Hospital staff must be present whenever pictures are taken.

Where a photograph contains sensitive personal data, it will generally be necessary for the individual being photographed to give their explicit consent to the photograph being taken and they should also be notified of all of the purposes for which the photograph will be used.

Personal cameras, including camera facilities on personal mobile devices, must not be used for any clinical purpose nor must they be used for the storing of clinical images however the clinical images were captured. Only Camera equipment purchased by the Trust specifically for clinical use may be used.

5.5 BYOD Service

Page 10 of 23
Mobile Device Policy, Version 5 -May 2013

Current version is held on the policy section of the intranet
The BYOD service allows any substantive Trust Employee with an approved mobile device the option to use their personal mobile device as a business tool.

5.6 Instant Messaging (IM)

Trust issued Smartphone’s and compatible BYOD devices will all be given access to the Trusts corporate Instant Messaging service. Staff will be able to access this service using their AD login credentials. The service is available at Whiston and St Helens Hospital. The service is provided to enhance communication between Staff. Staff should note that care should be taken when sending personal or sensitive information using the STHK HIS corporate Instant Messaging Service.

The Trust is providing Instant Messaging Services to improve communications and phase out all Non-Emergency Pagers. Selected bleeps may however remain in place for a limited time. Instant Messaging will be the preferred method of communicating for staff based at Whiston and St Helens Hospitals. By using the Trusts corporate Instant Messaging Service you agree (if you carry one) to surrender your non-emergency pager once the Instant Messaging application is in use Trust wide.

The Informatics Service retains a copy of all Instant Messages received or sent for a period of 12 months. The Department will not use this facility to monitor individual employees Instant Messaging traffic without written permission or unless they have a justified need to monitor or investigate an employee’s Instant Messages.

The routine retrieval is of historical messages is not a service that Health Informatics will provide.

5.7 Network:

STHK HIS will ensure that all Trust provided mobile devices have wireless network connectivity as follows;

Connectivity via the COIN wireless network where available

Connectivity via the mobile wireless network of the provider currently identified as providing voice and/or 3G services to the Trust which provides the best speed and coverage and the most reliable service within the constraints of value for money.
3G mobile data contracts can be supplied with devices for a pre-determined period and cost. The User is responsible for the contract payment and any additional; charges above contract data limits.

BYOD Devices will be given a connection to the trust Wireless Network. BYOD users (on application) will be issued with a secure username and password to access the wireless network.

5.8 Tariffs:

It should be noted that receiving data on a personal mobile device may incur a financial cost to you. It is advisable that you check with your personal mobile provider for more information regarding data plans and tariffs.

For Trust device users a number of tariffs are available offering 3G data connectivity for a monthly rental fee. STHK HIS will review tariffs on a regular basis to ensure that it remains the most competitive. The User will be informed of the mobile tariff on device acceptance.

If you are connected to the BYOD service your device will use the Wireless Network at no cost to you.

When connected to the BYOD Network or the VOIP service you are expected to abide by the Trusts Acceptable Use policy which references appropriate usage of phones.

5.9 Mobile Devices

STHK will offer a limited range of handsets and mobile devices, based on a technical assessment of reliability, price and ease of use. Allocation of some handsets/devices may be restricted based on staff role. STHK HIS will review this choice on a regular basis to ensure that the most competitive, functional and reliable equipment is available for staff.

5.10 Trust Provided Apple Mobile Devices

Apple iTunes

Apple App store functionality will be available for users of devices to purchase and install applications using their personal apple ID. Users without an Apple ID will be supported in registering an Apple ID on receipt of the device.

No corporate funding of any app store purchases will be provided. Health Informatics will provide a list of recommended, and appropriate, business applications.

Users will be responsible for any copyright or infringement of iTunes terms and conditions.
5.11 Device Security Settings

You must configure a PIN lock on any Trust issued mobile device.

Any smartphone/tablet e.g. Blackberry, iPad must be configured to lock after 5 minutes of inactivity and have a password set. This password must conform to the Trust Password Policy.

The device will be configured to wipe after 10 failed password attempts this will apply to Trust provided and BYOD devices.

Smartphones, laptops etc. must be encrypted to the Advanced Encryption Standard with a 256bit key.

5.12 Use of Personal Devices

Informatics has the capability to offer access to the Trust email system via the Internet.

5.13 Outlook Web Access

Allows you to access Microsoft Outlook in a web browser from your home computer.

Access to Outlook Web Access is available to all Trust staff by default at the URL: https://mail.shk.nhs.uk/

You must only access Outlook Web Access from a computer adequately protected against malware. This means running an up to date anti-virus programme with the latest operating system security updates installed. You must not access Trust email from a system which may be compromised e.g. PCs in an Internet Café may have key loggers or screen recorders installed unknown to you.

5.14 ActiveSync

Allows you to synchronize your Trust email with a mobile phone or tablet e.g. iPhone or iPad.

Only registered users may connect their personal phone or tablet to the Trust email system. You can register by raising a call with the IT Helpdesk and telling us your:

Username, Telephone Number, IMEI Number, Type of device

When you add your account to your device it will be initially “quarantined”. Informatics will check the device against the list of registered devices before enabling access.

Only devices which support full file system 256bit encryption are permitted to be connected. Informatics will maintain a list of permitted devices on the

Current version is held on the policy section of the intranet
Intranet. If you believe your device meets the encryption requirements and is not in the list you can raise a call for Informatics to consider adding the device to the list.

Any device connected via ActiveSync will have a security policy assigned which you must agree to before connection is permitted. The security settings enforced by the policy are:

- An 8 character password consisting of letters & numbers or symbols
- An automatic screen lock after 5 minutes of inactivity
- The ability for Informatics to remote-wipe the device

The 8 Character passwords have been reduced to a 4 digit pin on Smartphone's and Tablets. This is to allow greater usability of these devices.

5.15 Private / Personal data

Mobile devices provided by the Trust, are to be used primarily for business purposes. Only corporate data stored in email and group folder access is data protected.

Health Informatics managed Apple iPad devices have unrestricted iTunes functionality. Users install applications and store personal media and documents at their own risk. Any faults or IT support interventions may involve loss of any personal data.

Personal use must conform to the Trust Acceptable Use Policy

5.16 Data Backup of Personal information

Apple app store purchases are available to download again from app store.

You can backup any personal media and documents on Apple devices using the iTunes backup processes. The backup must be encrypted (this is enforced by policy on Trust issued devices).

5.17 Ordering Process

Applications for a Trust provided mobile device, or to connect a personal mobile device, should be made to the IT Help Desk on

0151 676 5678 or via the web form at: http://shkwebapps/itrequestform/

The Help Desk will guide the applicant through the application process, including how to obtain the necessary approvals and acknowledge the appropriate policies using the form in Appendix A of this policy.

The Help desk can advise on the standard lead time for delivery.
Applications will be periodically audited to ensure that there is a genuine continuing need for a mobile device, which cannot be met, by other forms of communications technology.

5.18 Damaged Mobile Devices

Mobile devices in need of repair should be returned to STHK HIS who will return them to the supplier for repair or replacement under warranty. It should be noted that manufacturers’ warranties do not normally cover damage caused by misuse or neglect and that the cost of such repairs will be borne by the user responsible.

The STHK HIS will make best endeavours to ensure a suitable replacement is issued as quickly as possible.

6. EQUALITY ANALYSIS

The Trust has a duty as a public body to publish all completed Equality Analysis Screening and Assessments. Please forward a copy of your completed proforma to Annette.craghill@sthk.nhs.uk – the Trust Patient and Workforce Equality Lead

The Patient and Workforce Equality Lead will conduct an audit on all completed Screening and Assessments every six months.

For advice in respect of answering the above questions, please contact the Patient and Workforce Equality Lead (Ext 7609)

<table>
<thead>
<tr>
<th>Equality Analysis Stage 1 Screening</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Title of Policy</strong></td>
</tr>
<tr>
<td><strong>Policy Author (s)</strong></td>
</tr>
<tr>
<td><strong>Lead Executive</strong></td>
</tr>
<tr>
<td><strong>Policy Sponsor</strong></td>
</tr>
<tr>
<td><strong>Target Audience</strong></td>
</tr>
<tr>
<td><strong>Document Purpose</strong></td>
</tr>
<tr>
<td><strong>Please state how the policy is relevant to the Trusts general equality duties to:</strong></td>
</tr>
<tr>
<td>• Eliminate discrimination</td>
</tr>
<tr>
<td>• Advance equality of opportunity</td>
</tr>
<tr>
<td>• Foster good relations</td>
</tr>
<tr>
<td><strong>List key groups involved or to be involved in the policy development (e.g. staff side representatives, service</strong></td>
</tr>
</tbody>
</table>

Page 15 of 23
Mobile Device Policy, Version 5 - May 2013

Current version is held on the policy section of the intranet
If in any doubt please consult with the Patient and Workforce Equality Lead

Does the policy **significantly** affect one group **less** or **more** favourably than another on the basis of: answer ‘yes/no’ (please add any qualification or explanation to your answer particularly if you answer yes)

<table>
<thead>
<tr>
<th>Yes/No</th>
<th>Comments/Rationale</th>
</tr>
</thead>
<tbody>
<tr>
<td>Race/ethnicity</td>
<td>No</td>
</tr>
<tr>
<td>Disability (includes learning disability, physical or mental disability and sensory impairment)</td>
<td>No</td>
</tr>
<tr>
<td>Gender</td>
<td>No</td>
</tr>
<tr>
<td>Religion / belief (including non belief)</td>
<td>No</td>
</tr>
<tr>
<td>Sexual orientation</td>
<td>No</td>
</tr>
<tr>
<td>Age</td>
<td>No</td>
</tr>
<tr>
<td>Gender reassignment</td>
<td>No</td>
</tr>
<tr>
<td>Pregnancy and maternity</td>
<td>No</td>
</tr>
<tr>
<td>Marriage and civil partnership</td>
<td>No</td>
</tr>
<tr>
<td>Career status</td>
<td>No</td>
</tr>
<tr>
<td>Will the policy affect the human rights of any of the above protected groups?</td>
<td>No</td>
</tr>
<tr>
<td>If you have identified potential discrimination, and there are any exceptions valid, legal and or justifiable?</td>
<td>No</td>
</tr>
<tr>
<td>If you have identified a negative impact on any of the above protected groups, can the impact be avoided or reduced by taking different action?</td>
<td>No</td>
</tr>
<tr>
<td>How will the effect of the policy be reviewed after implementation?</td>
<td>N/A</td>
</tr>
</tbody>
</table>
If you have entered ‘yes’ in any of the above boxes you **must** contact the Patient and Workforce Equality Lead (ext 7609 annette.craghill@sthk.nhs.uk) to discuss the outcome and ascertain whether a **Stage 2 Equity Analysis Assessment** must be completed.

<table>
<thead>
<tr>
<th>Name of the manager completing assessment: (must be one of the authors)</th>
<th>David McKee</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job title of manager completing the assessment</td>
<td>Assistant Director - ICT</td>
</tr>
<tr>
<td>Date of completion</td>
<td>September 5th, 2012</td>
</tr>
</tbody>
</table>

### 7. TRAINING

The use of mobile devices will be demonstrated by the IT Engineer delivering the device. Instructions on the use of the VPN client will be provided with any VPN tokens delivered.
Appendix A – Acceptance form

Acceptance form

<table>
<thead>
<tr>
<th>Device Model:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Department:</td>
<td></td>
</tr>
<tr>
<td>Issued To:</td>
<td></td>
</tr>
</tbody>
</table>

- I acknowledge receipt of an STHK HIS supported mobile device.
- I agree to abide by the requirements of the Mobile Device policy document. Before using the device in the event that I do not agree with the policy document, having read it, I agree to return the mobile device.
- I acknowledge my liability for the cost of any 3G contract and excess data charges made.
- I acknowledge any personal information is not the responsibility of the Health Informatics Service to recover.

Signed:

Printed:

Date:
Appendix B – BYOD Terms & Conditions

Bring Your Own Device (BOYD) Service Terms and Conditions
By bringing your own mobile device into work for the purposes of accessing St Helens and Knowsley NHS Trust Health Informatics Services (STHK HIS) BYOD service, you agree to the following terms and conditions of use:

- STHK HIS will allow staff members to view and access their email, calendar, contacts and access the corporate instant messaging service, staff will also be able to access the internet using a secure Wi-Fi connection from their personal mobile device.

- Members of staff must be aware that the responsibility for the actual device remains with them. The IT Helpdesk nor the Trust Network team will not provide any technical assistance to staff with issues with their own mobile devices, even where those devices have been authorised to be used for Trust business purposes.

- The Trust reserves the right to wipe all information from a member of staff’s mobile device should they deem it necessary, this will wipe all information from the device completely – this includes both corporate and personal information (contacts, messages, photo’s, apps, etc.) By accepting this Terms and Conditions document you are giving your explicit consent for the Trust to wipe your mobile device if it deems necessary.

- Staff members MUST inform the ICT service desk IMMEDIATELY if their mobile device is lost or stolen.

- Should a member of staff’s mobile device be required for any investigation into a member of staff’s conduct, the mobile device requested will be surrendered immediately to the Trust’s Information Governance team once the request has been made.

- STHK HIS are providing Instant Messaging Services to improve communications and phase out all Non-Emergency Pagers. Selected bleeps may however remain in place for a limited time. Instant Messaging will be the preferred method of communicating for staff based at Whiston and St Helens Hospitals. By using the Trust’s corporate Instant Messaging Service you agree (if you carry one) to surrender your Non-Emergency Pager once the Instant Messaging application is in use Trust-wide.

- Staff should note that care should be taken when sending personal or sensitive information using the STHK HIS corporate Instant Messaging Service.
• The Trust reserves the right to withdraw access to the BYOD services at any time.

• By agreeing to these Terms and Conditions you are explicitly stating that you understand that STHK HIS, or the Trust as a whole, will accept NO legal liability for any unlawful activity conducted on the mobile device in question.

• By accepting these Terms and Conditions you are explicitly stating that you have read, understood and accepted the Trust’s Mobile Device Policy, and will adhere to the provisions made within it.

Current version is held on the policy section of the intranet
Appendix C – BYOD Loan Mobile Phone Agreement

Mobile Phone Loan Phone Agreement

Terms & Conditions of Loan
- The Phone is on loan from St Helens & Knowsley Health Informatics Service (STHKHIS)
- The phone will remain the property of STHKHIS throughout the period of the loan and will be loaned for a period of 7 Days Only
- By accepting this device you must still adhere to the provisions made within the Trust's Mobile Device Policy and BYOD terms & Conditions.

Collection and Delivery
- A mutually agreed time/location will be arranged for the loan phone to be collected or delivered and returned after the 48 hour loan period.
- On return the device will be assessed for damages and all Asset tags examined

Recipients Responsibilities
- As the recipient you agree to guard the phone against loss, damage and theft.
- Operate the phone within operating guidelines and for the purpose it was designed.
- Ensure that identification marks or labels on the equipment are not removed, defaced, amended, and obscured including those which identify the equipment as belonging to STHKHIS.

Personal Liability
- You must ensure the device is returned to STHKHIS in the same condition it was issued, this will be checked by the IT Engineer
- In the event that the phone is lost or damaged beyond economical repair you agree to pay the cost of an iPhone 4S in full

Acceptance

Recipient I have read and accept the loan mobile phone agreement

Print Name……………………………………PayrollNumber………………Date………………

Signature…………………………………… Time………………

IT Engineer Sign and date on receipt of loan mobile phone

Print Name……………………………………

Signature……………………………… Date………………

Page 21 of 23
Mobile Device Policy, Version 5 -May 2013

Current version is held on the policy section of the intranet
Loan Phone Asset Number ..........................Loan PhoneSerialNumber......................

IT Engineer please make a note of any marks or scratches before and after the loan period

**Before Loan**

![Before Loan](image)

**After Loan**

![After Loan](image)
<table>
<thead>
<tr>
<th><strong>Type of Document</strong></th>
<th>Corporate Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Code:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Policy Sponsor</strong></td>
<td>Neil Darvill, Director of Informatics, Senior Information Risk Owner</td>
</tr>
<tr>
<td><strong>Lead Executive</strong></td>
<td>Neil Darvill, Director of Informatics</td>
</tr>
<tr>
<td><strong>Recommended by:</strong></td>
<td>Informatics Management Committee</td>
</tr>
<tr>
<td><strong>Date Recommended:</strong></td>
<td>12/06/2013</td>
</tr>
<tr>
<td><strong>Approved by:</strong></td>
<td>Information Governance Steering Group</td>
</tr>
<tr>
<td><strong>Date Approved:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Author(s):</strong></td>
<td>Stephen Brooks, Network Manager</td>
</tr>
<tr>
<td><strong>Date issued:</strong></td>
<td>June 2016</td>
</tr>
<tr>
<td><strong>Target audience:</strong></td>
<td>All staff</td>
</tr>
</tbody>
</table>

**Document purpose**

The purpose of this policy is to outline the remote access to computer systems and resources in the Trusts. The guidelines in this policy exist to protect the Trusts and its employees.

**Training requirements**

All staff must attend Mandatory Training in line with Trust Policy as the Information Security Policy is incorporated into this programme.

**Associated documents and Key References**

Acceptable Use Policy (January 2011)
Information Governance Policy (March 2012)
Corporate Records Management Policy (January 2010)
Data Protection Policy (June 2011)
Freedom of Information Policy (October 2009)
Information Risk Policy (June 2011)
Safe Haven Policy (April 2010)
Staff Disclosure Under FOI Policy (January 2009)
Trust Consent Policy (April 2011)
Disciplinary Policy and Procedure (July 2011)
Confidentiality Code of Conduct Policy (July 2012)
Access to Health Records Policy (January 2010)
Information Security Policy (September 2012)

**Financial Implications**

Failure to fully implement this policy could
result in monetary penalties being issued to the Trust by the Information Commissioners Office

### Consultation, Communication

<table>
<thead>
<tr>
<th>Consultation Required</th>
<th>Authorised By</th>
<th>Date Authorised</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analysis of the effects on equality</td>
<td>Craig Walker</td>
<td>June 2013</td>
<td>Approved</td>
</tr>
<tr>
<td>External Stakeholders</td>
<td>N/A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trust Staff Consultation: Assistant Director for Informatics</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Caldicott Guardian</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Implementation Plan

**Describe the Implementation Plan for the Policy (and guideline if impacts upon policy)**
Considerations include: launch event, awareness sessions, communication / training via Divisions and other management structures, etc.

<table>
<thead>
<tr>
<th>Timeframe for implementation?</th>
<th>RAG</th>
<th>Who is responsible for delivery?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Policy will be uploaded onto Intranet
  - Submitted for uploading when Policy Approved
  - Author

- Global Communication to alert staff of new policy
  - After Policy is uploaded
  - Author

- Staff will be made aware of policy when receiving Corporate Induction and Mandatory Training
  - Continuous
  - Line Manager, Training Team
### Performance Management of Policy KPI's  (Expected Outcomes)

<table>
<thead>
<tr>
<th>Describe Key Performance Indicators (KPIs) expected outcomes</th>
<th>How will the KPI be Monitored?</th>
<th>Which Committee will Monitor this KPI?</th>
<th>Frequency of Review</th>
<th>Lead</th>
</tr>
</thead>
<tbody>
<tr>
<td>Duties are carried out as described in the policy</td>
<td>Audit</td>
<td>IG Steering Group</td>
<td>Annually</td>
<td>IG Manager</td>
</tr>
<tr>
<td>Compliance will be monitored via the Information Governance Toolkit</td>
<td>IG Toolkit Submission</td>
<td>IG Steering Group</td>
<td>6 monthly</td>
<td>IG Manager</td>
</tr>
<tr>
<td>External Audit Rating to be of an acceptable standard.</td>
<td>External Audit</td>
<td>Audit Committee</td>
<td>Annually</td>
<td>IG Manager</td>
</tr>
</tbody>
</table>

### Performance Management of minimum NHSLA processes for this policy. Learning from Experience

<table>
<thead>
<tr>
<th>Who is responsible for producing action plans if deficits in KPI'S and associated processes identified</th>
<th>Which Committee will monitor these action plans</th>
<th>Frequency of Review</th>
</tr>
</thead>
<tbody>
<tr>
<td>IG Manager</td>
<td>IG Steering Group</td>
<td>Annually</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>How does learning occur?</th>
<th>Who responsible for implementing and disseminating learning information</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mandatory Training</td>
<td>IG Manager</td>
<td>In line with corporate timetable</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Archiving including retrieval of archived document</th>
<th>By whom will policy be archived and retrieved</th>
</tr>
</thead>
<tbody>
<tr>
<td>To be completed once version 4 approved</td>
<td>Web Team</td>
</tr>
</tbody>
</table>
## Document Version History

<table>
<thead>
<tr>
<th>Date</th>
<th>Author Designation</th>
<th>Summary of key changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>May 2012</td>
<td>01 Mark Williams</td>
<td>Document Created</td>
</tr>
<tr>
<td>May 2013</td>
<td>02 Stephen Brooks</td>
<td>Reviewed</td>
</tr>
<tr>
<td>June 2013</td>
<td>02 Stephen Brooks</td>
<td>Formatted</td>
</tr>
</tbody>
</table>
Policy Aim........................................................................................................p7

1. Introduction ........................................................................................................p7
2. Policy Objectives ...............................................................................................p7
3. Policy Definitions ................................................................................................p7
4. Duties, Accountabilities and Responsibilities .................................................p8
5. Policy Specific Procedures ...............................................................................p9
6. Equality Analysis ...............................................................................................p11
7. Training & Awareness ......................................................................................p12
8. Appendices .........................................................................................................p13
   a. Remote Access User Form ........................................................................p14
Executive Summary

Policy Aim:
The Remote Access Policy is meant to ensure the integrity and privacy of the Trusts data.

Policy Description:
The guidelines in this policy exist to protect the Trusts and its employees. This policy applies to all staff, student, temporary employees, and other personnel within the Trusts, including employees of affiliated third-party organisations. This policy applies to all equipment that is owned, leased, operated, or maintained by the STHKHISS.

1. Introduction

St Helens and Knowsley Health Informatics (STHKHISS) is committed to ensuring the privacy of the trusts, its employees, and its partners from unauthorised, illegal, and malicious actions by individuals, intentionally or otherwise.

- The STHKHISS recommends the use of its VPN when possible for accessing Trusts resources from off-campus.
- Workstation security is the responsibility of both STHKHISS support personnel and the workstation users.

2. Policy Objectives

- The purpose of this policy is to outline the remote access to computer systems and resources in the Trusts.
- This policy applies to all equipment that is owned, leased, operated, or maintained by the STHKHISS.
- Remote access implementations that are covered by this policy include, but are not limited to, dial-in modems, ISDN, ADSL (Broadband), VPN and cable modems, etc.

3. Policy Definitions

Cable Modem: Cable companies such as Telewest Broadband provide Internet access over Cable

TV coaxial cable. A cable modem accepts this coaxial cable and can receive data from the Internet at over it. Cable is currently available only in certain Area’s.

Dial-in Modem: A peripheral device that connects computers to each other for sending communications via the telephone lines. The modem modulates the digital data of computers into analog signals to send over the telephone lines, then demodulates back into digital signals to be read by the computer on the other end; thus the name “modem” for modulator/demodulator.
**Dual Homing:** Having concurrent connectivity to more than one network from a computer or network device. Examples include: Being logged into the corporate network via a local Ethernet connection, and dialling into BT or other Internet service provider (ISP). Being on a Trusts-provided Remote Access home network, and connecting to another network, such as a spouse's remote access. Configuring an ISDN router to dial into the Trusts network and an ISP, depending on packet destination.

**ISDN:** There are two flavours of Integrated Services Digital Network or ISDN: BRI and PRI. BRI is used for home office/remote access. BRI has two "Bearer" channels at 64kbit (aggregate 128kb) and 1 D channel for signalling info.

**Remote Access:** Any access to Trusts resources through a non-Trust controlled network, device, or medium.

**Split-tunnelling:** Simultaneous direct access to a non-Trusts network (such as the Internet, or a home network) from a remote device (PC, PDA, WAP phone, etc.) while connected into Trust's network via a VPN tunnel. VPN Virtual Private Network (VPN) is a method for accessing a remote network via "tunnelling" through the Internet.

**Non Trust Devices:** Personal Laptops PDA’s, Mobile Phones including iPods.

### 4. Duties Accountabilities and Responsibilities

#### 4.1 Chief Executive
The Chief Executive as the Accounting Officer for the Trust has ultimate responsibility for ensuring that this Policy is implemented.

#### 4.2 The Senior Information Risk Owner (SIRO)
The Director of ICT is the designated SIRO for the Trust and will be accountable for the delivery of this Policy and related work programmes;

#### 4.3 Health Informatics Service (STHKHIS)
The Health Informatics Service must approve all remote access accounts

#### 4.4 All Staff
Must apply to the Health Informatics Service to get a remote access account.

It is the responsibility of employees, contractors, vendors and agents with remote access privileges to STHKHIS resources on the Trusts network to ensure that their remote access connection is given the same consideration as the user’s on-site connection.

Employees and contractors with remote access privileges must ensure that their computer or workstation, which is remotely connected to
Trusts resources on the Trusts network are under complete control of the user.

5. Policy Specific Procedures

5.1 All hosts that are connected to STHKIS resources on the Trusts network via remote access technologies must use the most up-to-date anti-virus software; this includes Laptops.

5.2 The most recent security patches must be installed on the computer using the remote access connection.

5.3 Organisations or individuals who wish to implement non-standard Remote Access solutions to the Trusts resources via remote access must obtain prior approval from STHKIS.

5.4 The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of the Trusts authorised to engage in any activity that is illegal under law while utilising the STHKIS-owned resources.
The lists below are by no means exhaustive, but attempt to provide a framework for activities that fall into the category of unacceptable use.
- At no time should any employee provide their login or email password to anyone, not even family members
- Dual Homing or split-tunnelling while connected to Trusts Resources on the Trusts network is not permitted at any time.
- At no time should any non Trust owned equipment be connected remotely or otherwise.

Any machine found to be not following this policy will not be allowed to connect to the Trusts network.
6. Equality Analysis
### Equality Analysis Stage 1 Screening

<table>
<thead>
<tr>
<th>Title of Policy:</th>
<th>Remote Access Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Author(s):</td>
<td>Craig Walker</td>
</tr>
<tr>
<td>Lead Executive:</td>
<td>Neil Darvill</td>
</tr>
<tr>
<td>Policy Sponsor</td>
<td>Sandra Siwiak</td>
</tr>
<tr>
<td>Target Audience</td>
<td>All staff</td>
</tr>
</tbody>
</table>

**Document Purpose:**

- Please state how the policy is relevant to the Trusts general equality duties to:
  - eliminate discrimination
  - advance equality of opportunity
  - foster good relations

**List key groups involved or to be involved in policy development (e.g. staff side reps, service users, partner agencies) and how these groups will be engaged**

- Trust communication tools (Team brief, global emails)

**NB** Having read the guidance notes provided when assessing the questions below you must consider:

- Be very conscious of any indirect or unintentional outcomes of a potentially discriminatory nature
- Will the policy create any problems or barriers to any protected group?
- Will any protected group be excluded because of the policy?
- Will the policy have a negative impact on community relations?

If in any doubt please consult with the Patient and Workforce Equality Lead

**Does the policy significantly affect one group less or more favorably than another on the basis of:** answer ‘Yes/No’ (please add any qualification or explanation to your answer particularly if you answer yes)

<table>
<thead>
<tr>
<th></th>
<th>Yes/No</th>
<th>Comments/Rationale</th>
</tr>
</thead>
<tbody>
<tr>
<td>Race/ethnicity</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>Disability (includes Learning Disability, physical or mental disability and sensory impairment)</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>Gender</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>Religion/belief (including non-belief)</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>Sexual orientation</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>Age</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>Gender reassignment</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>Pregnancy and Maternity</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>Marriage and Civil partnership</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>Carer status</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>Will the policy affect the Human Rights of any of the above protected groups?</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>If you have identified potential discrimination, are there any exceptions valid, legal and/or justifiable?</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>If you have identified a negative impact on any of the above protected groups can the impact be avoided or reduced by taking different action?</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>How will the effect of the policy be reviewed after implementation?</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>If you have entered yes in any of the above boxes you must contact the Patient and Workforce Equality Lead (ext 7609/ <a href="mailto:Annette.craghill@sth.k.nhs.uk">Annette.craghill@sth.k.nhs.uk</a>) to discuss the outcome and ascertain whether a Stage 2 Equality Analysis Assessment must be completed.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| Name of manager completing assessment: (must one of the authors) | Craig Walker |
| Job Title of Manager completing assessment | Information Governance Manager |
| Date of Completion: | May 2013 |

7. Training & Awareness

The HIS recognises that to gain the commitment of staff to support and meet local security requirements they must be aware of and understand why various procedures are in place.

- IG Training detailing the security of systems will be provided
- IT training for system access will be provided by the HIS IT trainers

Staff responsibilities for preservation of confidentiality, Data Protection and security must be identified in the Trust’s contracts of employment and terms and conditions and should be reinforced in local induction and subsequent training in Information Governance standards.

Computer facilities must only be used for authorised business. Non-business or unauthorised personal use by staff without management approval will be regarded as possible cause for disciplinary action by that organisation.
The Trust will ensure that all users of the network are provided with the necessary security guidance, awareness and appropriate training to discharge their security responsibilities.

All users of the network will be made aware of the contents and implications of this Network Security Policy and (where appropriate) network security procedures.

Irresponsible or improper actions by users may result in disciplinary action(s).

### 8. Appendices

This policy should be read in conjunction with other relevant Information Governance policies, in particular:

- Information Governance Policy;
- Information Security Policy;
- Acceptable Use Policy;
- Mobile Device Policy;
- Email & Internet Policy.
- Network Security Policy

These and other policies ensure the Trust complies with relevant laws and NHS guidance, including:

- Copyright, Designs & Patents Act 1988;
- Access to Health Records Act 1990;
- Computer Misuse Act 1990;
- The Data Protection Act 1998;
- The Human Rights Act 1998;
- Electronic Communications Act 2000;
- Freedom of Information Act 2000;
- Health & Social Care Act 2001;
- NHS Confidentiality Code of Practice;
Remote Access policy User Acceptance Form

I ........................................................................................................................................................................
Confirm that I have received a copy of the Remote Access Policy and will abide by the Policy.

Signed:- .................................................................

Job Title:- .................................................................

Department:- .................................................................

Date:- .................................................................

Authorised:- .................................................................

RSA Fob Number:- ................................................................. Exp Date:-
.................................................................