MOBILE DEVICES POLICY

Policy Author(s) | STHK – Network Manager
---|---
Accountable Manager(s) | STHK – Director of Informatics
Ratified by (Committee/Group) | NHS Halton CCG Integrated Governance Committee
Date Ratified | 05/01/2015
Target Audience | All staff, including contractors and volunteers
Review Date | 17/04/2018

This Policy has been developed by St Helens and Knowsley Health Informatics Service (HIS), who act as NHS Halton CCG’s IT Service Provider.

This policy has been approved and adopted by NHS Halton CCG and is applicable to all staff, including contractors and volunteers.

VERSION HISTORY

<table>
<thead>
<tr>
<th>Issue Date</th>
<th>Version No</th>
<th>Brief Description of Change</th>
<th>Changed by</th>
</tr>
</thead>
<tbody>
<tr>
<td>17/04/2015</td>
<td>6</td>
<td>Updated</td>
<td>STHK</td>
</tr>
</tbody>
</table>
Mobile Device Policy

Document Summary

This policy sets out the criteria for issue of Trust provided mobile devices and devices that utilize the wireless network Service, the rules around their use, use of personal devices by staff, and acceptable use of Mobile devices on Trust premises by patients/visitors.

<table>
<thead>
<tr>
<th>DOCUMENT NUMBER</th>
<th>STHK 0124</th>
</tr>
</thead>
<tbody>
<tr>
<td>APPROVING COMMITTEE</td>
<td>Information Governance Steering Group</td>
</tr>
<tr>
<td>DATE APPROVED</td>
<td>17/04/2015</td>
</tr>
<tr>
<td>DATE IMPLEMENTED</td>
<td>Date of Approval</td>
</tr>
<tr>
<td>NEXT REVIEW DATE</td>
<td>3 Years of approval</td>
</tr>
<tr>
<td>ACCOUNTABLE DIRECTOR</td>
<td>Director of Informatics</td>
</tr>
<tr>
<td>POLICY AUTHOR</td>
<td>Network Manager</td>
</tr>
<tr>
<td>TARGET AUDIENCE</td>
<td>All Staff</td>
</tr>
<tr>
<td>KEY WORDS</td>
<td>Mobile Phones, Tablets, Remote Access, active sync, Wearable tech,</td>
</tr>
</tbody>
</table>

Important Note:

The Intranet version of this document is the only version that is maintained.

Any printed copies should therefore be viewed as “uncontrolled” and, as such, may not necessarily contain the latest updates and amendments.
## Contents

1 SCOPE ................................................................................................................................. 3
2 Introduction .............................................................................................................................. 3
3 Statement of Intent .................................................................................................................. 3
4 Definitions ................................................................................................................................. 3
5 Duties Accountabilities and Responsibilities ................................................................. 4
   5.1 Management Responsibilities ....................................................................................... 4
   5.2 Staff Responsibilities ..................................................................................................... 5
6 Qualifying Criteria for Trust Supplied Mobile Devices .................................................. 6
   6.1 Compliance ...................................................................................................................... 6
   6.2 Trust staff must ............................................................................................................... 6
   6.3 Mobile Devices in Acute Trust Buildings ................................................................. 7
   6.4 Mobile Devices and Driving ......................................................................................... 7
7 Use of recording devices ......................................................................................................... 8
8 BYOD Wireless Service ......................................................................................................... 8
9 Instant Messaging (IM) ........................................................................................................... 8
10 Network ................................................................................................................................. 9
11 Mobile network Tariffs ......................................................................................................... 9
12 available Mobile Devices ...................................................................................................... 9
   12.1 Trust Provided Apple Mobile Devices (Apple iTunes) .............................................. 10
   12.2 Device Security Settings ............................................................................................ 10
13 TRAINING ............................................................................................................................ 12
14 MONITORING COMPLIANCE WITH THIS DOCUMENT ........................................ 13
15 RELATED TRUST POLICY/PROCEDURES .......................................................... 13
Appendix 1 ................................................................................................................................. 14
Appendix 2 – Acceptance form ............................................................................................... 16
Acceptance form ....................................................................................................................... 16
Appendix 3 – BYOD Terms & Conditions ............................................................................. 17
Appendix 4 – BYOD Loan Mobile Phone Agreement ............................................................ 19
1 SCOPE

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 and acceptable use of mobile devices by patients and visitors.

2 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 the issuing 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.

3 STATEMENT OF INTENT

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

4 DEFINITIONS

**Mobile device** in this context is any mobile electronic device capable and/or used for communication i.e. phone, smartphone, pager, any portable computer e.g. laptop, tablet, iPad®, iphone®, 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.

**Virtual private network (VPN)** allows users to connect to the STHK COIN and it resources securely over the public network (internet.)
Bring Your Own Device (BYOD) refers to the use of personal mobile devices to access NHS Services through the Trust network.

**Instant Messaging (IM)** 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.

**Recording devices:** devices capable of recording and/or storing audio, video and still images.

### 5 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 approved mobile devices and of personal devices allowed to connect to the Trust and its resources.

- Ensuring that a loan phone 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.

- Ensure that the employee has surrendered their Trust provided mobile phone and is using their own personal device in its place

#### 5.1 Management Responsibilities

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

- Ensure their staffs have a legitimate business need for a Trust issued device or BYOD connection as well as ensuring that the mobile device is been used as a business tool.

- 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 mobile devices they authorised and signed for by their member of Staff if that device becomes lost, stolen or damaged beyond economical repair.

5.2 Staff Responsibilities

To read and understand the mobile device and associated polices before requesting for a Trust issued device or BYOD connection.

Ensure you comply with the requirements of this and other associated policies.

To take good care of the mobile device and take all reasonable precautions to ensure that Trust issued devices are not damaged, lost or stolen. In the event that your Trust issued or BYOD device is lost or stolen, staff must raise an Incident Report, report the theft to the police and obtain an incident number and contact IT helpdesk.

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.

• Tel: 01516765678

• E-mail: IT.Helpdesk@sthk.nhs.uk

Staff must ensure that a personal device presented for BYOD access has not modified the security settings implemented by the manufacturer or service provider/carrier. E.G. jail broken or rooted.

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 device.

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. Your device must be secured in a case at all times.

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 wireless service must inform the IT Helpdesk so that their device can be removed from the system.

The Informatics Service will perform a system clean-up on BYOD devices not seen on the Network for a 6 month period. Any such devices will be removed from the system.

6 QUALIFYING CRITERIA FOR TRUST 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

6.1 Compliance

This policy relates to the 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.

6.2 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.

6.3 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 devices 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.

• Wearable technology capable of recording still and/or moving image with or without sound recording capabilities without written authorisation is not permitted within Acute Trust buildings.

6.4 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 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.

# USE OF RECORDING DEVICES

The use of recording devices in hospital is restricted to respect patient confidentiality, privacy and dignity. Recording devices, not limited to audio, video and still facilities on mobile devices, are not allowed in secluded areas such as toilets, bathrooms and treatment rooms. Authorisation has to be obtained from a senior member of staff in order for patients and visitors to take a photograph.

Where a recording might contain or contains sensitive personal data, it will generally be necessary for the individual being recorded to give their explicit consent before the recording starts or used and they should also be notified of all of the purposes for which the recording will be used.

Personal recording devices, 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 document. Only Camera equipment purchased by the Trust specifically for clinical use may be used.

# BYOD WIRELESS SERVICE

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.

# INSTANT MESSAGING (IM)

Trust issued mobile device and compatible BYOD devices can be given access to the Trusts corporate Instant Messaging service upon request. 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 (bleeps). 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.

10 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 internet data (3G/4G) services to the Trust which provides the best speed and coverage and the most reliable service within the constraints of value for money.

Internet data (3G/4G) mobile data contracts can be supplied with devices for a predetermined 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.

11 MOBILE NETWORK 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 mobile 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 code of confidentiality policy and other associated policies which references appropriate usage of mobile device.

12 AVAILABLE 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.

12.1 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.

Personal/confidential/sensitive work related data must not be stored in third party cloud storage such as iCloud®.

12.2 Device Security Settings

- You must configure a Password/PIN lock on any mobile device (BYOD and Trust issued device) that is connected to the Trust network resources or Trust VPN soft token installed.

- Any portable mobile device e.g. Blackberry, iPad® must be configured to lock after 3 minutes of inactivity and have a password set. This password must conform to the Trust Password standard.

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

- Mobile devices must be encrypted to the Advanced Encryption Standard (AES) with a minimum of 256bit encryption.

- In exceptional circumstances the length of the password characters will be reduced to a minimum of four. This will have to be approved by the Director of Informatics or his deputies.

Use of Corporate Email on Personal Devices

- Informatics has the capability to offer access to the Trust email system via the public network (Internet).

Outlook Web Access
- 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 public networks/computer or 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.

**ActiveSync**

Allows you to synchronize your Trust email with a BYOD or Trust issued devices.

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 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:

- A 9 character password consisting of letters & numbers or symbols
- An automatic screen lock after 3 minutes of inactivity
- The ability for Informatics to remote-wipe the device
- With authorisation from the SIRO or equivalent the 9 character passwords can be reduced to a 4 digit pin on mobile devices. This is to allow greater usability of these devices.

**Private / Personal data**

Mobile devices provided by the Trust from the COPE category, will 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 this policy and other associated policies

**Data Backup of Personal information**

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

You can back-up 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 and BOYD devices).

**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/](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 2 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.

**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 or department responsible for the loss or damaged mobile device.

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

**13 TRAINING**

The use of Trust issued mobile devices will be demonstrated by the IT Engineer delivering the device. Instructions on the use of the VPN client will be provided during the delivery of the VPN token by the IT engineer.
14 MONITORING COMPLIANCE WITH THIS DOCUMENT

Monitoring if compliance with this document will be overseen by the Information Governance Steering Group.

Key performance indicators of the Policy

<table>
<thead>
<tr>
<th>Describe Key Performance Indicators (KPIs) Must reflect</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>Annually</td>
<td>IG Manager</td>
</tr>
<tr>
<td>Compliance will be monitored via the Information Governance Toolkit</td>
<td>6 Monthly</td>
<td>IG Manager</td>
</tr>
<tr>
<td>External Audit Rating to be of an acceptable standard.</td>
<td>Annually</td>
<td>IG Manager</td>
</tr>
</tbody>
</table>

Performance Management of the Policy

<table>
<thead>
<tr>
<th>Aspect of compliance or effectivenes s being monitored</th>
<th>Monitoring method</th>
<th>Individual responsible for the monitoring</th>
<th>Frequency of the monitoring activity</th>
<th>Group / committee which will receive the findings / monitoring report</th>
<th>Group / committee / individual responsible for ensuring that the actions are completed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Refer to KPIs</td>
<td>Spot checks</td>
<td>IG Manager</td>
<td>As Above</td>
<td>IG Steering Group</td>
<td>Risk Management Council</td>
</tr>
<tr>
<td></td>
<td>IG Toolkit 314-2a</td>
<td></td>
<td></td>
<td>Risk Management Council</td>
<td>Trust Board</td>
</tr>
<tr>
<td></td>
<td>Mandatory Training</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>IG Toolkit Reports External Audit Reports</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IG Mandatory Training</td>
<td>Training will be monitored in line with the Induction Mandatory and risk Management Training Policy.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

15 RELATED TRUST POLICY/PROCEDURES
• Network and information Security and Risk Policy
• Information & Governance Policy
• Confidentiality code of conduct Policy
• H&S policies (Pat testing Chargers)
• Asset management policy

APPENDIX 1

Equality Analysis

“St Helens and Knowsley Teaching Hospitals NHS Trust is committed to creating a culture that promotes equality and embraces diversity in all its functions as both an employer and a service provider. Our aim is to provide a safe environment, free from discrimination, and a place where all individuals are valued and are treated fairly. The Trust adheres to legal requirements and seeks to mainstream the principles of equality and diversity through all its policies, procedures and processes.

The Trust takes a zero tolerance approach to all forms of discrimination, harassment and victimisation and will make every effort to ensure that no patient or employee is disadvantaged, either directly or indirectly, on the basis that they possess any of the “protected characteristics” as defined by the Equality Act 2010. The protected characteristics are as follows: - race; disability; sex; religion or belief; sexual
orientation; gender reassignment; marriage and civil partnership; pregnancy and maternity; and age.

This policy will be implemented with due regard to these commitments.

All authors of policy documents must include a completed equality analysis Stage 1 screening. Policy authors must refer to the Trust Equality and Diversity Policy 2011 and the equality analysis toolkit and associated guidance documents (Stage 1 and Stage 2) available on the intranet.

Equality Analysis for this policy

<table>
<thead>
<tr>
<th>Equality Analysis Stage 1 Screening</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Title of Policy:</td>
</tr>
<tr>
<td>2 Policy Author(s):</td>
</tr>
<tr>
<td>3 Lead Executive:</td>
</tr>
<tr>
<td>4 Policy Sponsor</td>
</tr>
<tr>
<td>5 Target Audience</td>
</tr>
<tr>
<td>6 Document Purpose:</td>
</tr>
<tr>
<td>7 Please state how the policy is relevant to the Trusts general equality duties to: eliminate discrimination advance equality of opportunity foster good relations</td>
</tr>
<tr>
<td>8 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</td>
</tr>
</tbody>
</table>

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

9 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></th>
<th>Yes/No</th>
<th>Comments/ Rationale</th>
</tr>
</thead>
<tbody>
<tr>
<td>Race/ethnicity</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Disability (includes Learning Disability, physical or mental disability and sensory impairment)</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Gender</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Religion/belief (including non-belief)</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Sexual orientation</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Age</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>--------------</td>
<td>----</td>
<td></td>
</tr>
<tr>
<td>Gender reassignment</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Pregnancy and Maternity</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Marriage and Civil partnership</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Carer status</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>1 0 Will the policy affect the Human Rights of any of the above protected groups?</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>1 1 If you have identified potential discrimination, are there any exceptions valid, legal and/or justifiable?</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>1 2 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>
<td></td>
</tr>
<tr>
<td>1 3 How will the effect of the policy be reviewed after implementation?</td>
<td>The policy will be audited at least annually in line with the key performance indicators</td>
<td></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 Equality Analysis Assessment must be completed.

Name of manager completing assessment: (must one of the authors) Tony Atherton
Job Title of Manager completing assessment Network Manager
Date of Completion: 02 – December - 2014

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

**APPENDIX 2 – ACCEPTANCE FORM**

**ACCEPTANCE FORM**

<table>
<thead>
<tr>
<th>Device Model:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Department:</td>
</tr>
<tr>
<td>Issued To:</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 internet data (3G/4G) services /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 3 – 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 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.

- 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 reject and/or 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
APPENDIX 4 – 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………………………..…Payroll Number…………………………….

Date……………………………………Signature……………………………………

Time……………………………………

IT Engineer Sign and date on receipt of loan mobile phone

Print Name……………………………………
Signature……………………. Date……………………

Loan Phone Asset Number …………………………………………………

Loan Phone Serial Number………………………………………………

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

<table>
<thead>
<tr>
<th>Before Loan</th>
<th>After Loan</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1" alt="Before Phone" /></td>
<td><img src="image2" alt="After Phone" /></td>
</tr>
<tr>
<td><img src="image3" alt="Before Phone" /></td>
<td><img src="image4" alt="After Phone" /></td>
</tr>
</tbody>
</table>