## Policy Checklist

<table>
<thead>
<tr>
<th>Name of Policy:</th>
<th>Bring Your Own Device Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose of Policy:</td>
<td>Bring Your Own Device (BYOD) is a component of the Trust’s Technology Enabled Change (TEC) strategy to adopt best of breed IT to support clinical work. A key value of the Trust is to promote creativity and innovation, developing new approaches to meeting needs, promoting best practice, supporting modernisation and reform.</td>
</tr>
<tr>
<td>Directorate responsible for Policy</td>
<td>Directorate of Performance and Reform</td>
</tr>
<tr>
<td>Name &amp; Title of Author:</td>
<td>Stephen Hylands, Head of Information Technology</td>
</tr>
<tr>
<td>Does this meet criteria of a Policy?</td>
<td>Yes</td>
</tr>
<tr>
<td>Trade Union consultation?</td>
<td>Yes</td>
</tr>
<tr>
<td>Equality Screened by:</td>
<td>Stephen Hylands, Head of Information Technology</td>
</tr>
<tr>
<td>Date Policy submitted to Policy Scrutiny Committee:</td>
<td>16th December 2013</td>
</tr>
<tr>
<td>Members of Policy Scrutiny Committee in Attendance:</td>
<td>Vivienne Toal, Head of Employee Engagement &amp; Relations (Chair), Melanie McClements, Assistant Director of Older People’s Services, Claire Graham, Head of Corporate Records (for Siobhan Hanna), Marita Magennis, Head of Social Work and Social Care Governance, Fiona Wright, Assistant Director of Nursing Governance, Daphne Johnston, Clinical &amp; Social Care Governance Manager</td>
</tr>
<tr>
<td>Policy Approved/Rejected/Amended</td>
<td>Amended to include; ICO advice for BYOD implementation, clarification on employee eligibility and responsibilities.</td>
</tr>
<tr>
<td>Policy Implementation Plan included?</td>
<td>Yes</td>
</tr>
<tr>
<td>Any other comments:</td>
<td></td>
</tr>
<tr>
<td>Date presented to SMT</td>
<td></td>
</tr>
<tr>
<td>Director Responsible</td>
<td>Mrs Paula Clarke</td>
</tr>
<tr>
<td>SMT Approved/Rejected/Amended</td>
<td></td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---</td>
</tr>
<tr>
<td>SMT Comments</td>
<td></td>
</tr>
<tr>
<td>Date received by Employee Engagement &amp; Relations for database/Intranet/Internet</td>
<td>16 December 2013</td>
</tr>
<tr>
<td>Date for further review</td>
<td>2 year default</td>
</tr>
</tbody>
</table>
# POLICY DOCUMENT – VERSION CONTROL SHEET

| **Title** | Title: Bring Your Own Device Policy  
Version: 1.3  
Reference number/document name: |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Supersedes</strong></td>
<td>None</td>
</tr>
</tbody>
</table>
| **Originator** | Name of Author: Stephen Hylands  
Title: Head of Information Technology |
| **Scrubtny Committee & SMT approval** | Referred for approval by:  
Date of Referral:  
Scrubtny Policy Committee Approval (Date)  
SMT approval (Date) |
| **Circulation** | Issue Date:  
Circulated By:  
Issued To: As per circulation List (details below) |
| **Review** | Review Date: December 2015  
Responsibility of (Name): Stephen Hylands  
Title: Head of Information Technology |
Southern Health and Social Care Trust

BRING YOUR OWN DEVICE (BYOD) Policy

Informatics Department
October 2013
Version 1.3
Contents

1.0 INTRODUCTION.........................................................................................................................1
2.0 PURPOSE AND AIMS..............................................................................................................1
3.0 BYOD POLICY STATEMENT..................................................................................................1
4.0 SCOPE OF POLICY...............................................................................................................3
5.0 RESPONSIBILITIES..............................................................................................................3
6.0 DEVICE & USER SUPPORT ..................................................................................................4
7.0 MANAGEMENT AND STAFF LIABILITY ..............................................................................4
8.0 CONCLUSION.........................................................................................................................5
9.0 EQUALITY AND HUMAN RIGHTS CONSIDERATIONS......................................................5
10.0 ALTERNATIVE FORMATS....................................................................................................5
11.0 COPYRIGHT.........................................................................................................................6
12.0 SOURCES OF FURTHER ADVICE.......................................................................................6
1.0 INTRODUCTION

1.1 Bring Your Own Device (BYOD) is a component of the Trust’s Technology Enabled Change (TEC) strategy to adopt best of breed IT to support clinical work. A key value of the Trust is to promote creativity and innovation, developing new approaches to meeting needs, promoting best practice, supporting modernisation and reform.

1.2 Innovation by its very nature produces more risk and BYOD is not immune to this. This policy addresses these new risks and mitigates their impact whilst not stifling the positive impact they will have.

1.3 Allowing clinicians and other staff to use personal devices that they already use on a regular basis in the work environment is an innovative part of the answer. Bring Your Own Device (BYOD) as part of an agile working concept can help drive efficiencies, with the ability to facilitate smoother workflows, promote team collaboration and help boost staff satisfaction.

1.4 This Policy has been developed in accordance with the Trusts Key Principles for Policy Development.

2.0 PURPOSE AND AIMS

2.1 Bring Your Own Device (BYOD) is a component of the Trust’s Technology Enabled Change (TEC) strategy to adopt best of breed IT to support clinical work. A key value of the Trust is to promote creativity and innovation, developing new approaches to meeting needs, promoting best practice, supporting modernisation and reform.

2.2 The implementation of BYOD aims to allow staff to choose to access Trust email, calendar and Sharepoint, using their own device, thus avoiding the need for staff to carry more than one mobile IT device.

2.3 Ensure that all processing of personal data on the BYOD device is under Trust control and is compliant with the Data Protection Act (1998).

3.0 BYOD POLICY STATEMENT

3.1 Mobile Device Management (MDM) software
Allows IT Security Team to configure, secure, monitor and wipe smartphones and tablets. The chosen MDM platform (AirWatch) will be used to manage the Trust BYOD environment.

3.2 BYOD Device Type

Due to the sheer number of smart phone devices available it is not possible to allow any or every arbitrary smartphone or tablet onto the Trust network (all devices need to be tested with MDM software). A relatively broad range of platforms e.g. Android, iPhone and BlackBerry will be facilitated but in the first instance only Apple iOS (iPhone/iPAD) will be connected. Android devices will be enabled following manufacturer and O/S version testing. An approved list of BYOD devices will be posted onto SharePoint following sign-off by the IT Security Team.

3.3 BYOD Security

Security concerns over privacy and leakage or loss of sensitive data on employee owned devices are addressed in this BOYD policy. The Mobile Device Management (MDM) software selected to manage the BYOD devices will implement the following security parameters :-

- Pin access codes on all BYOD devices will have a minimum of 6 characters enforced (default is 4) – with an alphanumeric value. An enforced change will be pushed out every 60 days following enrolment.
- An encrypted container will be created on all personal devices which will be managed by the IT Security Team; the encrypted container will store attachments/corporate data only. This encrypted container will only be accessed by the Trust employee, via their Trust password.
- Data cannot be moved from the encrypted container into the BYOD device e.g. email data cannot be cut & pasted from Trust email into native email client on the device.
- The encrypted container will be remotely wiped in the event of loss of the device (user agrees to advise Trust IT Helpdesk as soon as is practicable of loss) or when staff leave the Trust.
- A complete wipe maybe carried out on a lost device upon request by staff – default will be encrypted container wipe only.
- IT Security Team has the right to create a Blacklist of Apps that may be blocked on BYOD devices in order to maintain the security and integrity of the Trust’s IT Infrastructure.
- Trust IT Security staff will not monitor or interfere with personal data on a non-corporate BYOD device.
- The Trust cannot be held liable for loss of personal applications or data, whether directly or indirectly resulting from the use of Trust apps and
or the wiping of such apps or data (staff should backup personal data/photographs etc before signing up to BYOD).

- A jailbreaking, rooting or the equivalent and making modifications to device hardware or O/S beyond routine installation of updates as provided by the device maker are strictly prohibited and would be treated as a hacking attempt.
- Ability to save screen capture to the device memory will be denied.
- Use of Speech Interpretation & Recognition Interface (SIRI) software will be denied when the screen is locked.
- An enforced security screen lock will be enabled on all BYOD devices with default time set to 1 minute to prevent unauthorised access.

4.0 SCOPE OF POLICY

4.1 The BYOD Policy applies to all staff who wish to use a non corporate device within the work environment and are licensed to do so.

4.2 Due to the cost associated with BYOD (licence costs) not all staff are eligible for BYOD. For those staff choosing to use BYOD, rationalisation of corporate devices will be required. Authorised staff will have access to corporate email, calendar and SharePoint in the first instance. Access to further Trust applications and information systems may be provided in the future, when fully tested and robust assurances on data protection gained.

4.3 Due to current licensing and financial constraints; in the first instance access will be provisioned for all Junior Doctors. Rollout to other medical and clinical staff across the Trust will be on a case by case basis.

5.0 RESPONSIBILITIES

5.1 First and foremost, it is vital to specify which functions a given user can access, and what general behaviours are acceptable. It’s important to protect the Trust from users who may have, for example, illicit materials on their devices, or information that may be proprietary to another firm.

5.2 Whilst the Trust is concerned with maintaining security on BYOD devices, staff maybe worried about preserving the convenience they need in order to work from their mobile device, and the privacy they expect regarding personal information on the device. The MDM solution provides employees with the privacy they need while maintaining the required level of corporate protection.
5.3 The use of camera, browsers, Bluetooth will not be limited on the device; however staff should not use the device contrary to the Trust IT Security Policy; Trust Data Protection Policy or the Data Protection Act 1998. Staff should adhere to the following acceptable use principles:

- Any device enrolled in Trust BYOD use must not be loaned to anyone else (all BYOD devices are synchronised with user network accounts).
- Whilst the Trust does not apply acceptable user policies in relation to Internet access, browsing or Social Media on BYOD devices staff should be mindful of and abide by Data Protection legislation and patient confidentiality.
- If a user attempts to change BYOD security settings the IT Security Team will be notified via the MDM software and will disable the user.

5.4 The BYOD policy assumes that access to the corporate network will be based on user 3G/4G contract basis and not Trust Wi-Fi access (due to limited Wi-Fi coverage outside acute sites and impact on network bandwidth).

- There will be no reimbursement for staff using personal devices to access corporate network; BYOD facilitates access only.
- There will be no reimbursement for costs associated with SMS use, Internet access or voice costs.

5.5 The device remains under the ownership of the user and all costs associated with personal use will remain the responsibility of the user. Users should consider their own voice and data use - the Trust does not assume any financial responsibility associated with the BYOD device.

6.0 DEVICE & USER SUPPORT

6.1 The use of BYOD device for corporate access is solely at the risk of the user and the Trust does not provide any support or helpdesk assistance with the use of such devices. Initial setup guide/instructions will be provided to all users who are eligible for BYOD.

7.0 MANAGEMENT AND STAFF LIABILITY

7.1 A custom End User License Agreement (EULA) will be developed as part of the deployment of the MDM, during enrolment for BYOD staff will be prompted to read and accept before enabling their personal device. This is an important feature for legal and liability management regarding BYOD. The end user agreement will require user acceptance of:-
• IT Security Team administrator permissions to manage the device

• User obligations in the event of a lost or stolen device

• Acknowledgment that the device will be enabled with proprietary corporate data and is subject to Trust security policies regarding sensitive data.

• Agreement to abide by the Trust BYOD Policy; IT Security Policy; Data Protection Policy and the Data Protection Act 1998.

7.2 The Trust will not assume control over the devices themselves and instead focus on access controls and limiting risks such as leaving corporate data on BYOD devices.

8.0 CONCLUSION

8.1 This Policy will empower staff to bring their own devices to improve productivity, collaboration and mobility. It will protect sensitive information from loss and theft while addressing privacy, compliance and risk management mandates. It will simplify management through self-service provisioning, scenario-based policies and automated management and monitoring.

9.0 EQUALITY AND HUMAN RIGHTS CONSIDERATIONS

9.1 This policy has been screened for equality implications as required by Section 75 and Schedule 9 of the Northern Ireland Act 1998. Equality Commission guidance states that the purpose of screening is to identify those policies which are likely to have a significant impact on equality of opportunity so that greatest resources can be devoted to these.

Using the Equality Commission's screening criteria, no significant equality implications have been identified. The policy will therefore not be subject to an equality impact assessment.

Similarly, this policy has been considered under the terms of the Human Rights Act 1998, and was deemed compatible with the European Convention Rights contained in the Act

10.0 ALTERNATIVE FORMATS
10.1 This document can be made available on request in alternative formats, e.g. plain English, Braille, disc, audiocassette and in other languages to meet the needs of those who are not fluent in English.

11.0 COPYRIGHT

11.1 The supply of information under the Freedom of Information does not give the recipient or organisation that receives it the automatic right to re-use it in any way that would infringe copyright. This includes, for example, making multiple copies, publishing and issuing copies to the public. Permission to re-use the information must be obtained in advance from the Trust.

12.0 SOURCES OF FURTHER ADVICE

12.1 Line Managers should be contacted in the first instance, in relation to any specific queries on Policy content. Line Managers should then escalate queries which they are unable to address, to the Policy Author.

12.2 Information relating to BYOD guidelines and the Data Protection Act can be accessed from the Information Commissioner’s Office (ICO) via the following link: