

## REPORT TO MERTON CLINICAL COMMISSIONING GROUP GOVERNING BODY

**Date of Meeting:** 24 March 2016

**Agenda No:** 7.6

**Attachment:** 11

<b>Title of Document:</b> Merton CCG Updated Non-Clinical Policies	<b>Purpose of Report:</b> To request that the Governing Body approve the non-clinical policies detailed in this report.
<b>Report Author:</b> David Cotter - Principal Associate Corporate Affairs (South East Commissioning Support Unit)	<b>Lead Director:</b> Andrew Hyslop, Chief Finance Officer Merton CCG
<b>Executive Summary:</b> SEE OVERLEAF	
<b>Key Sections for particular note:</b> Whole document	
<b>Recommendation(s):</b> The Governing Body is asked to: <ol style="list-style-type: none"> <li>1. <b>SUPPORT</b> a three year review cycle for the above policies</li> <li>2. <b>APPROVE</b> the following updated policies on the recommendation of the Audit and Governance Committee:             <ul style="list-style-type: none"> <li>o Policy for Policy Development</li> <li>o Conflicts of Interest Policy</li> <li>o Procurement Policy</li> <li>o Risk Management Policy</li> <li>o Non-Clinical Incident and Near Miss Policy</li> </ul> </li> <li>3. <b>APPROVE</b> the following updated policies on the recommendation of the Senior Information Responsible Officer:             <ul style="list-style-type: none"> <li>o Application Security Policy</li> <li>o Bring your Own Device Policy</li> <li>o ICT Emergency Preparedness Response and Resilience Policy</li> <li>o ICT Change Policy</li> <li>o Device Encryption Policy</li> <li>o Network, Applications and Internet Acceptable Use Policy</li> <li>o Procurement, Replacement and Disposal Policy</li> <li>o ICT Security Policy</li> <li>o Registration Authority (RA) Policy</li> <li>o RA Smartcard Use Policy</li> </ul> </li> </ol> <p>Electronic copies of the Policies were sent to all Governing Body members with the meeting papers. They will also be accessible via the CCG's website as part of the GB papers.</p>	
<b>Committees which have previously discussed/agreed the report:</b> Audit and Governance Committee 17 March 2016 (not ICT policies)	
<b>Financial Implications:</b> None	
<b>Implications for CCG Governing Body:</b> None	
<b>How has the Patient voice been considered in development of this paper:</b> N/A	

<b>Other Implications:</b> N/A
<b>Equality Assessment:</b> N/A
<b>Information Privacy Issues:</b> None – consistent adoption and application of these policies will enhance information privacy
<b>Communication Plan: (including any implications under the Freedom of Information Act or NHS Constitution)</b> Once approved the updated policies will be notified to all CCG staff and placed on the CCG Intranet.

<p><b>Executive Summary:</b></p> <p><b>1. Polices Presented for Approval on the Recommendation of the Audit and Governance Committee</b></p> <p>The Terms of Reference of the Audit and Governance Committee charge the Committee to annually review the non-clinical policies of the CCG and make appropriate recommendations to the Governing Body (paragraph 6.6.3). In accordance with this the following updated policies were presented for review to the Audit and Governance Committee on 17 March 2016:</p> <ul style="list-style-type: none"> <li>• Policy for Policy Development</li> <li>• Conflicts of Interest Policy</li> <li>• Procurement Policy</li> <li>• Risk Management Policy</li> <li>• Non-Clinical Incident and Near Miss Policy</li> </ul> <p>After discussion the Audit and Governance Committee agreed to recommend approval of the policies to the Governing Body on the recommendation of the Committee.</p> <p><b>2. Information and Communications Technology (ICT) Polices Presented for Approval on the Recommendation of the Senior Information Risk Owner (SIRO)</b></p> <p>Merton CCG has appointed the Chief Finance Officer as SIRO. The SIRO will review the following updated ICT policies before the Governing Body meeting on 24 March 2016 and anticipates making a recommendation that the Governing Body approve the policies on his recommendation:</p> <ul style="list-style-type: none"> <li>• Application Security Policy</li> <li>• Bring your Own Device Policy</li> <li>• ICT Emergency Planning and Business Continuity Policy</li> <li>• ICT Change Policy</li> <li>• Network, Applications and Internet Acceptable Use Policy</li> <li>• Procurement, Replacement and Disposal Policy</li> <li>• ICT Security Policy</li> <li>• Device Encryption Policy</li> <li>• Registration Authority (RA) Policy</li> <li>• RA Smartcard Use Policy</li> </ul> <p>The South East Commissioning Support Unit (SECSU) is the provider of an end to end ICT solution for Merton CCG, other CCGs, to a number of third party providers upon which CCGs depend and a provider of ICT services to SECSU itself which also provides other services to CCGs. This means that SECSU recommends the consistent adoption of its ICT policies across all service providers and as such these policies are put forward as SECSU policies which are relevant to both SECSU and all the organisations who are their customers. Merton CCG has consistently supported the view that this approach was the best way to minimise risk and maintain control of the local ICT infrastructure.</p> <p><b>3. Policy Review Cycle</b></p> <p>A policy review cycle of 3 years is suggested for all policies; this would not preclude earlier or more frequent review if there was a need.</p>
--

# Merton CCG Updated Non-Clinical Policies

## 1. Introduction

A number of non-clinical policies have been reviewed since the last Governing Body meeting or are due for review before the Governing Body meeting on 24 March 2016. The policies fall into two categories:

- Policies presented for approval on the recommendation of the Audit and Governance Committee
- Information and Communications Technology (ICT) Policies presented for approval on the recommendation of the Senior Information Risk Owner (SIRO)

As part of the review exercise a review period of 3 years is recommended for all policies. This does not preclude earlier review if needed.

## 2. Policies Presented for Approval on the Recommendation of the Audit and Governance Committee

The Terms of Reference of the Audit and Governance Committee charge the Committee to annually review the non-clinical policies of the CCG and make appropriate recommendations to the Governing Body (paragraph 6.6.3). In accordance with this the following updated policies were presented for review to the Audit and Governance Committee on 17 March 2016:

- Policy for Policy Development
- Conflicts of Interest Policy
- Procurement Policy
- Risk Management Policy
- Non-Clinical Incident and Near Miss Policy

The policies were presented for cyclical review and additionally for the following reasons:

Policy for Policy Development	To reflect the current Constitution (November 2015) and Governing Body Committee's Terms of Reference.
Conflicts of Interest Policy	<p>In response to two of the recommendations in the January 2016 Internal Audit Conflicts of Interest (COI) Audit Report:</p> <ul style="list-style-type: none"><li>• Management to ensure that supporting policies are referenced in the COI policy to explicitly state that they should be read in conjunction with one another and form part of the CCG's risk management framework. The amendment was made to section 3.2 of the Policy.</li><li>• Bribery Act 2010 responsibilities to be included within section 5 Principles and General Safeguards of the COI policy. The amendment was made to section 5.3 of the Policy.</li></ul>

Procurement Policy	In response to one of the recommendations in the January 2016 Internal Audit COI Audit Report: <ul style="list-style-type: none"> <li>The current Procurement Policy to be revised to include the requirement and process to maintain a register of procurement decisions. The amendment was made to section 9 of the Policy.</li> </ul>
Risk Management Policy	Minor changes were made to reflect the current CCG Governance structure, roles, responsibilities and operation.
Non-Clinical Incident and Near Miss Policy	Minor changes were made to reflect the current CCG Governance structure, roles, responsibilities and operation.

After discussion the Audit and Governance Committee agreed to recommend approval of the policies to the Governing Body on the recommendation of the Committee.

### **3. Information and Communications Technology (ICT) Policies Presented for Approval on the Recommendation of the Senior Information Risk Owner (SIRO)**

Merton CCG has appointed the Chief Finance Officer as SIRO. The SIRO will review the following updated ICT policies before the Governing Body meeting on 24 March 2016 and anticipates making a recommendation that the Governing Body approve the policies on his recommendation:

Application Security Policy	Defines required security standards for all applications and the management of incidents relating to application security.
Bring your Own Device Policy	Defines required standards for the use of non-organisation owned devices for work purposes.
ICT Emergency Planning and Business Continuity Policy	Defines required standards for emergency planning and maintaining service during and after a disaster.
Network, Applications and Internet Acceptable Use Policy	Defines required standards for access to be authorised to the organisation's network, applications or the internet.
Procurement, Replacement and Disposal Policy	Defines required standards for procurement, replacement and disposal of all ICT hardware and software.
ICT Security Policy	Defines required security standards for all elements of the organisation's network and ICT infrastructure and the management of security incidents.
Registration Authority Policy/ RA Smartcard Use Policy	Sets the principles for the management and use of Registration Authority (RA) functions which determines the issuing and use of smartcards that permit access to NHS Care Records Service (NHS CRS) applications

ICT Change Policy	Defines required standards for implementing change to applications or the infrastructure.
Device Encryption Policy	Covers all devices owned by or connected to the SECSU ICT Network at any site owned or leased by the organisation or from any site from which the SECSU provides these services.

The South East Commissioning Support Unit (SECSU) is the provider of an end to end ICT solution for Merton CCG, other CCGs, to a number of third party providers upon which CCGs depend and a provider of ICT services to SECSU itself which also provides other services to CCGs. This means that SECSU recommends the consistent adoption of its ICT policies across all service providers and as such these policies are put forward as SECSU policies which are relevant to both SECSU and all the organisations who are their customers. Merton CCG has consistently supported the view that this approach was the best way to minimise risk and maintain control of the local ICT infrastructure.

Effective ICT policy documentation enables Merton CCG to be fully prepared to adhere to legislative obligations and meet both local and national guidelines. They help to outline organisations objectives, codes of practice and standards, facilitating consistent decision making, quality of service and robust governance.

SECSU policies provide a structured approach to facilitate good working practices, ease of user access and clear governance processes. The documents will also support organisations when gathering evidence for compliance with the Information Governance Toolkit (IGT), a national requirement. SECSU has adopted the policies listed above and recommends a consistent adoption across its customer base.

#### 4. Policy Review Cycle

A policy review cycle of 3 years is suggested for all policies; this would not preclude earlier or more frequent review if there was a need.

#### 5. Conclusion

The Governing Body is asked to:

- **APPROVE** the following updated policies on the recommendation of the Audit and Governance Committee:
  - Policy for Policy Development
  - Conflicts of Interest Policy
  - Procurement Policy
  - Risk Management Policy
  - Non-Clinical Incident and Near Miss Policy
  
- **APPROVE** the recommendation to be made by the Senior Information Risk Owner in respect of the following policies:
  - Application Security Policy
  - Bring your Own Device Policy
  - ICT Emergency Preparedness Response and Resilience Policy

- ICT Change Policy
  - Device Encryption Policy
  - Network, Applications and Internet Acceptable Use Policy
  - Procurement, Replacement and Disposal Policy
  - ICT Security Policy
  - Registration Authority (RA) Policy
  - RA Smartcard Use Policy
- **SUPPORT** a three year review cycle for the above policies