Peterborough and Stamford NHS Foundation Trust and Hinchingbrooke Health Care Trusts

Infrastructure Review

14 September 2016

Version: v2.3
Status: Final [Redacted]
Authors: Michael Bone, Paul Cunningham & Clive Booth

Approvals

Version	Issue Date	Status	Reason for Issue
V0.3g	05/09/2016	Draft	1st Draft for Customer Review on 06/09/2016
V2.1	09/09/2016	Issue	Updated Costs
V2.2	13/09/2016	Issue	Updated Costs
V2.3	14/09/2016	Issue	Review and approval

Distribution

METHODS
ADVISORY

Shaping public services for the digital age

Names	Title	Date of Issue	Version
Jon Peate	Head of IT	05/09/2016	V0.3g
Barry Patton	IT Operations Manager	05/09/2016	V0.3g
Jon Peate	Head of IT	09/09/2016	V2.1
Jon Peate	Head of IT	13/09/2016	V2.2
Victoria Hughes	Principal Consultant	14/09/2016	V2.3

The principal point of contact for this report is:

Victoria Hughes
Methods Advisory Limited
16 St Martin's le Grand
London
EC1A 4EN

Phone: 020 7240 1121
Fax: 020 7379 8561
Email: victoria.hughes@methods.co.uk
www.methodsadvisory.co.uk

Contents

1. Executive Summary

The purpose of this Infrastructure Review was to examine the IT Infrastructure and an agreed number of supporting services ahead of the proposed merger between Peterborough and Stamford NHS Foundation Trust (PSHT) and Hinchingbrooke Healthcare NHS Trust (HHCT). It is clear that the Infrastructure at PSHT has greatly benefited from the building of the new Peterborough City Hospital and this is best demonstrated by the well-equipped and tidy IT data centres and network hub rooms. The PSHT IT team have a strong senior management group lead by an experienced Head of IT, who has recently taken over responsibility for IT at HHCT also.

Each Trust has a current IT Strategy document that sets out the plans the two Trusts have covering the period 2014 to 2017. The HHCT IT strategy was developed during a time when Circle Health ran the hospital and has not been updated since, whilst the PSHT IT Strategy was refreshed in early 2016. Each is aligned to the National IT Agenda with a focus on local service delivery as directed by their commissioners. However, that is where the similarities end, as PSHT has continued to invest in IT Infrastructure year on year, maintaining a good standard and recognising the value IT has as a key enabler of change. In contrast, the approach at HHCT has been to make only minimal investment often driven by a position where something critical has either already broken or is likely to do so in the near future. Where investment has been made, the IT Team have worked hard to maximise the benefits that the investment can yield, concentrating on critical components at the heart of the network and around the security perimeter.

In summary the areas of concern at HHCT are as follows:

- Primary data centre – not fit for purposes and needs immediate action
- Network hub rooms
    - 5 fail every time power is switched - needs immediate action
    - Remaining 18 hub rooms – very obsolete equipment, needs action soon
- Wired Network
    - 75 network connection devices are very obsolete
        - 10 units need immediate replacement
    - 65 units need replacing over the next 3 years
- Wireless Network
    - Operable but installed to an old standard, needs to be refreshed
- Network Management software
    - Would benefit from merger with more advanced PSHT solution
- Voice Services
    - No fall back if digital system collapses
    - Would benefit from small fall back system to sustain emergency phones
- Computing Devices
    - Only very modest investment in workstations over past three years
    - Need a one off capital investment (£320k) to replace very obsolete workstations
- Server Computing and Storage
    - Modest investment in additional computing provision is needed to sustain the existing service and the known future growth
    - HHCT only part way through upgrade to core storage solution, this needs to be completed quickly to ensure sufficient capacity exists to support the merger, clinical systems consolidation and adequate disaster recovery.

Unified Communications is a fast growing area across Information Technology as businesses, including healthcare organisations, seek to integrate communications technology to deliver easy to use and seamless access to information, resources and people. We noted the recent eComms Project to look at Unified Communications and, given the findings of the Outline Business Case, would suggest that as part the new service model design, IT should be engaged with clinicians and managers to determine how such technologies can be used to improve cross-site working and drive up efficiencies.

One of the core IT Solutions is electronic mail and here the two Trust have a notable difference. PSHT has its own local solution built around the leading commercial solution, whilst HHCT has the NHS national solution. The debate about the way forward for e-mail consumed many hours and to provide assurance, additional views where sought from thought leaders both in the NHS and outside. The conclusion is that the Trust would gain the greatest benefit, as it looks to build more integrated Trust wide collaborative services, from an expansion of the local solution in use at PSHT. Due to the complexity that arises from this debate, a more detailed review of risks and benefits has been included in the review.

In every area that we have reviewed, we have documented risks where these exist, have provided options for partial or full resolution and, have included recommendations covering immediate action, tactical use covering the first 2-3 years of the merger process and, strategic recommendations that extend for five years by which time the merger should be complete. In each area where there is a cost we have, where ever possible, identified where capital (one off) funding will be required and where recurring funds will be needed. We have further divided sectional costs by separating costs for goods or services from the costs for people (Professional Services). A full breakdown of each is included in the report but in summary the costs (incl. VAT) are as follows:

	COSTS	
	Capital (One Off)	Revenue
TOTAL INFRASTRUCTURE COSTS FOR MERGED TRUST	**£2,449,850.03**	**£1,103,850.42**

Whilst we have noted a number of areas of concern above, we would also like to highlight some areas of best practice and indeed exemplary work found during the review. Each Trust has an IT Service Desk which acts as the primary interface for users and we have found very high levels of customer satisfaction, well beyond the NHS norm at both Trusts. In terms of Integration Services, both Trust have selected class leading solutions and the development of e-Track at PSHT is an exemplary example of this being exploited to the full. Finally, we were delighted to find IT Security at PSHT highly compliant with the International Standard (ISO:27001) and would advise that this again is an exemplary model that has been developed for safety of users and as a benefit to the Trust.

2. Introduction

On 24th May 2016 a formal proposal to merge Peterborough and Stamford Hospital NHS Foundation Trust with Hinchingbrooke Healthcare NHS Trust was reported. Both Boards of Directors agreed that an outline business case should be prepared to identify options, risks, benefits and costs, at a high level, for the merger. The basis for this business case is the acceptance that whilst Peterborough & Stamford Hospital NHS Foundation Trust is clinically sustainable, it is not financially sustainable and Hinchingbrooke Healthcare NHS Trust is neither. The outline business case has identified that by merging the two Trusts into one and, by redesigning many of its services, both business and clinical, it should be possible for the new Trust to reach both clinical and financial sustainability.

Also recognised by the business case is the need to streamline and automate many existing manual processes. As Information Technology is the key to technology enabled change, the Trust commissioned two pieces of consultancy work focussed on:

1. Infrastructure
2. Clinical Systems

Methods Advisory was awarded the first lot on Infrastructure and this report is the resulting Review.

2.1 Purpose

The purpose of the review has been to look at an agreed number of areas of Information Technology Infrastructure and to document the current position of each at both Peterborough & Stamford Hospital NHS Foundation Trust and Hinchingbrooke Health Care NHS Trust. The review was to identify:

- what each Trust has in place across the agreed areas
- the risks each area carries
- what needs to be addressed in order to facilitate the successful delivery of services in the merged Trust

For each risk or shortfall found, the review has also identified options to resolve, or at least mitigate, the risk and a cost in terms of capital investment and/ or revenue expenditure to deliver the option.

2.2 Scope

The scope of the Infrastructure work has focussed on the following areas:

- The physical estate including data centres and network hub rooms on both hospital sites
- The wired and wireless network used to deliver data, voice and video across the organisations
- The security of the network perimeter - current external links and what remote access is available, along with the management platforms used to monitor all of these digital communications services

In mind of the future, the review also looked at electronic presence and unified communications as these can greatly help in terms of collaborative working along with voice services, both analogue and digital, as well as paging and the switchboard service. For end users, the review has covered desktop/ laptop computing, all manner of mobile devices and the security required to keep them safe. Behind such technology, the review has also covered all of the server based compute, storage and core database technology across both Trusts including a detailed review of how resilient these services are and what fall back provision is available.

Key to Information Technology is its interface to its users, therefore the Service Desk has also been reviewed along with the electronic directory that binds them all together, including the provision of electronic mail. The review has also covered security including structures (Governance), standards, policy, procedures and reporting alongside technological resilience including business continuity and disaster recovery planning.

2.3 Exclusions

At the start of the engagement it was agreed that Microsoft licensing would be outside the scope of this review, however where these directly impinge on areas of agreed coverage, such as e-mail, this exclusion has been ignored.

3. Findings

3.1 Glossary of Terms

AD	Active Directory (Microsoft)
AP	Access Point
API	Application Programme Interface
BCI	British Continuity Institute
CCG	Clinical Commissioning Group
DC	Data Centre
EDM	Electronic Document Management
EWA	Enterprise Wide Agreement (Microsoft)
HHCT	Hinchingbrooke Healthcare NHS Trust
HH	Hinchingbrooke Hospital
HSCIC	Health and Social Care Information Centre
IP	Internet Protocol
IVR	Interactive Voice Response
LAN	Local Area Network
LDSD	LANDesk Services Desk
LDMS	LANDesk Management Suite
MDM	Mobile Devices Management
PAS	Patient Administration System
PCH	Peterborough City Hospital
PSHT	Peterborough and Stamford NHS Foundation Trust
PSTN	Public Switched Telephone Network
RFID	Radio Frequency Identification
SNMP	Simple Network Management Protocol
SIRO	Senior Information Risk Officer
SRH	Stamford and Rutland Hospital
TCP	Transmission Control Protocol
TIA	Telecommunications Industry Association
UPS	Uninterruptible Power Supply
VDC	Virtual Data Connection
VDI	Virtual Desktop Infrastructure
VoIP	Voice over IP
WAN	Wide Area Network
UC	Unified Communications

3.2 Physical Estates

3.2.1 Data Centres

🚦	**Immediate**	**Replace DC1 at Hinchingbrooke with Commercially Hosted Data Centre**
	Tactical	**Consider new Data Centre build as part of the Health Campus development**
	Strategic	**Align Data Centre capacity with requirements of the merged Trust's service offerings**

3.2.1.1 Current Position

PSHT

PCH has three data centres (DC), two classified as primary and a third classified as the development DC. Each of the primary data centres would be defined as being close to Tier 2 under the TIA standards document 942-2 (for reference, a summary of the data centre tiers is provided in Appendix A). Although a small number of minor items would complete the Tier 2 level. These include the provision of CCTV, and upgrade to the main lighting (to L3 level) and the provision of formal emergency lighting in particular above the main door. In addition, the provision of a local environmental monitoring station should be considered to provide immediate alerting to the IT Department should the environment change.

Both DC1 and DC2 have a high level of occupancy leaving only a modest amount of space for further development. However, DC3 is only lightly populated and has the advantage of being immediately adjacent to an IT Hub Room making it possible to remove the wall that separates the two to create a larger data centre. A number of modest upgrades around flooring, lighting, air conditioning and fire suppression would be needed to reach full Tier 2 compliance but this would provide space for a further 6 racks of expansion.

> Risks
> Whilst the Tier 2 standard denotes redundancy, a potential single point of failure exists in DC1 in that the water from both air conditioning units exits the room via a single pipe. Should this pipe be compromised, the air conditioning will cease working leading to thermal overload and equipment shutdown. The Trust is aware of this and so environmental monitoring has been installed to minimise this risk.
>
> All three data centres are lit by standard neon strip lights and none have any formal emergency lighting which means that they are below the standard with regard to light. Ideally the primary lighting should be to L3 level with emergency lighting, in particular above the main door. The Trust has included a re-chargeable torch to address this issue but in time the lighting provision should be considered for upgrade.
>
> Aside from these small items the data centres at PCH provide a very sound base upon which to build future services.

HHCT

HHCT has two data centres, one older DC in the main hospital (DC1) and one newer DC in the Treatment Unit (DC2). DC1 was not purpose built, starting life as the telephone frame room and being augmented from time to time as demands for data centre space grew. DC2 is more modern, was purpose built and, like the data centres at PCH, would be defined as being close to Tier 2 under the TIA standards document 942-2.

The construction and fitment of DC1 falls someway short of the Tier 2 standard. In terms of occupancy DC1 is already at maximum capacity in terms of computer racks and has only minimal expansion space available. In addition, the power feed to DC1 is operating at its maximum load capacity as is the UPS that provides short term back up power. As a result, DC1 has been on the HHCT risk register for some time and moving forward, should be downgraded to become a network hub room only.

By contrast DC2 carries a modest load and has sufficient capacity for a further 6 racks of expansion. There are a small number of exception issues, most notably, the inclusion of the batteries for the UPS being housed in the DC, the lack of CCTV and the same lighting issues as outlined above for PSHT.

Risks

DC1 presents a series of risks in terms of space, power provision and distribution, water ingress, environmental monitoring, lighting and basic construction. As a result, immediate action is required to address these risks and so options with costs are below:

3.2.1.2 Options

There are four options open to the Trust with regard to DC1 as follows:

<table>
<tr><td><b>1</b></td><td><b>Do Nothing</b></td></tr>
<tr><td colspan="2">The Trust could choose to do nothing and accept the risk. However, the Trust has already experienced a number of major outages across both its network and computer storage solutions and the continued use of DC1 does nothing to address this risk. In a post Trust merger configuration, the impact of losing DC1 would only increase the scale of the loss and the resulting impact on business and clinical services.

<b>On this basis the Do Nothing option is rejected</b></td></tr>
<tr><td><b>2</b></td><td><b>Purpose Build a Data Centre on Site</b></td></tr>
<tr><td colspan="2">Identify a suitable space within the hospital campus and build a fully compliant Tier 2 data centre. Whilst this would resolve the issues with DC1, space on site is at a premium and the cost of such a build (based on a 120 Sq. M footprint) would come close to £1,000,000 by the time dual power feeds and communications ducts are included.

<b>On this basis the Purpose Build option is rejected</b></td></tr>
<tr><td><b>3</b></td><td><b>Build a Data Centre as part of the Proposed Health Campus</b></td></tr>
<tr><td colspan="2">As part of the wider development of health services across Cambridgeshire a scheme has already been commissioned to develop the HHCT site into a multi-service Health Campus. As part of this development there is room within the scheme to include the construction of a data centre compliant with the Tier 2 standard. However, the timeline for any data centre development within the Health Campus is a minimum of 18 months away. Allowing time for construction and commissioning, live use would not commence for 2 years. In addition, the exact needs of the data centre would be difficult to specify as the business needs of the Health Campus will take some time to emerge. It is therefore highly difficult to generate a cost of the Health Campus option at this time.

<b>On this basis the Health Campus option is noted for possible future development</b></td></tr>
<tr><td><b>4</b></td><td><b>Use a Commercial Data Centre for Hosting</b></td></tr>
<tr><td colspan="2">The use of commercial hosting would see HHCT use a third party data centre built to at least the Tier 2</td></tr>
</table>

standard (but likely Tier 3) linked to the Trust network by dual resilient external links. The Trust would move a selected number of data racks into the hosting centre and continue to manage the delivery of computing services remotely. This model is already widely in use by healthcare organisations and is usually a highly cost effective way of providing high quality data centre capacity rather than building something on site.

It should also be noted that the use of a commercial hosting centre contract can be highly agile, allowing the Trust to scale up or down as its business needs change. As the new service model for the merged Trust is agreed and as the needs of the Health Campus emerge, the Trust would be able to exit the commercial hosting agreement and move into its own data centre, if this is agreed as part of the Health Campus. This flexibility allows the Commercial Hosting option to be used either as a tactical solution or to grow from being tactical to strategic as the nascent organisation grows.

On this basis the Commercial Hosting option is recommended

3.2.1.3 Costs

The costs associated with options 1-4 above are as follows:

Option	Title	Capital	Revenue
1	Do Nothing	£0.00	£0.00
2	Purpose build Data Centre (Note 1)	£1,200,000.00	£67,000.00
3	Build Data Centre as part of Health Campus (Note 2)	£750,000.00	£32,500.00
4	Use Commercial Data Centre for Hosting (Note 3)	£26,785.00	£302,504.23

Note 1: The capital and revenue costs of a full compliant Tier 2 data centre including dual routed duct work is an estimate based upon our experience of such work in new hospital builds elsewhere. Please note Tier 2 assumes this development to be part of an existing hospital building as a standalone data centre would cost considerably more.

Note 2: The capital and revenue costs of a full compliant Tier 2 data centre including dual routed duct work is an estimate based upon our experience of such work in new hospital builds elsewhere. They have been reduced by 25% as we assumed building structure costs has been included in the work already proposed for the health campus.

Note 3: The capital and revenue costs are based upon a non-competitive quotation and we believe that a lower revenue cost would be achieved through a competitive procurement.

3.2.1.4 Recommendations

Immediate: Downgrade DC1 from a data centre to a hub room, removing servers and storage to a Tier 2 or better compliant data centre. Retain the core network switch at this location and ensure that the environment, mechanical and electrical service are sufficient to mitigate all identified risks.

Identify a suitable commercial data centre provider and engage, by way of a hosting contract, a compliant data centre service to house the servers and storage migrated out of DC1. Ensure hosting contract is flexible and agile such that it can be amended as the nascent merged Trust service model takes shape.

Tactical: Review options for a data centre as part of the proposed Health Campus. If the option offers value for money and meets Tier 2 or above compliance, include new data centre as part of the Health Campus development.

Strategic: Review data centre options as the merge Trust develops, ensure data centres remain compliant and that capacity is aligned with the merged Trust service model.

3.2.2 Hub Rooms

🚦	**Immediate**	**Replace UPS equipment at 5 highlighted hub rooms at HH. Review need for fire suppression in key hub rooms**
	Tactical	**Initiate UPS equipment replacement programme at remaining 23 to mitigate down time risk**
	Strategic	**Ensure hub room equipment is maintained to minimise loss of service risks.**

3.2.2.1 Current Position

PSHT

Alongside the 3 Data Centres, PCH has a further 34 hub rooms that house more local IT equipment. Each room is equipped with a local UPS and one or more air conditioning units. The standard hospital fire detection system is included in the room and each room is secured by a physical key lock and/ or a card swipe. At this time, automatic fire suppression is not provided as standard in hospital hub rooms. However, there are occasions when a hub may grow to house sufficient technology to elevate its function to one that is considered business or even mission critical. This is most often found in key diagnostic areas like radiology or pathology. In such circumstances a local fire suppression solution may become a sound solution. Appendix B contains details of such a solution should the Trust deem it necessary.

In our opinion all of the hub rooms at PCH are suitable for continued use as part of a merged Trust.

HHCT

HH has some 23 hub rooms that house more local IT equipment. Each room is equipped with a local UPS and a small number have air flow or air conditioning units. The standard hospital fire detection system is included in the room and each room is secured by a physical key lock and/ or a card swipe. It should be noted that all 23 hub rooms either already have UPS equipment that is obsolete and has failed, or is end of life and likely to fail in the future.

None of the hub rooms have automatic fire suppression; however, there are occasions when a hub may grow to house sufficient technology to elevate its function to one that is considered business or even mission critical. Appendix B contains details of such a solution should the Trust deem it necessary.

Risks

At this time 5 hub rooms have been identified as having UPS equipment that is obsolete and so no longer provides short term power in the event of a failure. The outcome is a minimum period of 15 minutes IT and Telephone down time whenever power is lost or cycled. This includes all routine generator tests and all forms of planned/ unplanned electrical work in such locations. As a result, staff who work in such areas have to be aware of any routine or planned electrical work so that data is not lost and alternative means of communications are utilised; if users are unaware or forget, data can be lost.

The remaining 18 hub rooms also have UPS equipment that has reached end of life and have deteriorating battery life issues. If left unattended, in time these 18 units will fail and the impact outlined above will become hospital wide with far greater potential for lost data and equipment damage across the hub rooms.

3.2.2.2 Options

There is only one practical option and that is to commence a programme of planned replacement for obsolete and end of life UPS equipment. The need to start with the 5 failed units is urgent and so should start without delay, progress then needs to continue through the remaining 18 hub rooms until all UPS equipment is fully operational and capable of providing short term power for a period of not less than 30 minutes.

3.2.2.3 Costs

HHCT Estates Department have provided costs as follows:

Work Package	**Capital**	**Revenue**
Replace failed UPS in 5 hub rooms @ £4,000 each	£20,000.00	£2,000.00
Replace end of life UPS in 18 hub rooms @ £4,000 each	£72,000.00	£7,200.00
Total UPS Replacement Costs over 4 financial years	**£92,000.00**	**£23,600.00**

3.2.2.4 Recommendations

Immediate: Replace the 5 failed UPS units with new equipment and mitigate the impact of planned/ unplanned down time on IT systems, Telephone and end users across the hospital.

Tactical: Over Financial Years 17/18, 18/19 and 19/20 replace a further 6 UPS units per annum based upon a priority plan agreed with IT to mitigate the potential impact of planned/ unplanned down time on IT systems, Telephone and end users across the hospital.

Strategic: Review developing infrastructure needs at HHCT in-line with Trust IM&T Strategy 2014 – 2017 and direct infrastructure investment as needed to sustain a modern technology enabled health service.

3.3 Digital Communications

3.3.1 Wired Network

🚦	**Immediate**	**Replace 10 most obsolete Cisco Edge Network switches at HHCT**
	Tactical	**HHCT & PSHT - Continue to replace end of support Cisco [redacted] switches part of the rolling investment in infrastructure**
	Tactical	**Based on the Libretti Health report on Clinical Systems, deploy aggregation switch technology**
	Strategic	**Continue regular investment in network infrastructure Plan for upgrade to Cisco Core Switches at PSHT**

Appendix C includes a schematic showing a full four layered campus network with separate layers for: Data Centre, Core, Distribution and Edge networks. It is provided only as an exemplar of what makes up a full four-layer network design and so is used to put the descriptions provided of the various Trust networks into context for the reader.

3.3.1.1 Current Position

PSHT CORE

PCH comprises a classic 2-layer network build around high speed cores with a single core node located in each of the two data centres for performance and resilience [redacted] operating with a single supervisor card and an integrated wireless services module that acts as a controller for the Trust’s wireless network. Each core switch is fitted with dual power supply modules and is fed from the data centre UPS. The two core switches are joined using two separately routed 10Gb network links that form the core network. A further single 1Gb network link connects the core network to a third smaller [redacted] core network switch at SRH. All of the core network equipment is underpinned by a full maintenance and support contract that operates 24 x 7.

All three core network nodes are also connected directly to a local [redacted] for security (see perimeter for details) as well as having local network links at each site to the BT voice network (PSTN) and the NHS N3 network. Access to the Internet is by router over the NHS N3 network via the NHS Network Internet Relay. In the event that the single 1Gb link to SRH fails, voice and data traffic can continue to reach SRH over the PSTN and NHS N3 network.

At this time all servers are directly connected to one of the core switches based upon the DC in which they are located. There are no aggregation switches in use and none of the servers are dual homed. As a result, a single point of failure exists in terms of server connectivity.

> Risks
>
> Although the Trust has two core network switches, one in each DC, the use of a single direct connection from servers to the core means that there is a single point of failure should such a connection fail.

3.3.1.2 Options

There are two options open to the Trust with regard to this single point of failure as follows:

1	Do Nothing
The Trust could choose to do nothing and accept the risk. However, this would leave the Trust open to a potentially significant outage should either the link or local core switch fail. **On this basis the Do Nothing option is rejected**	
2	**Deploy Aggregation Switches**
Deploy a number of aggregation switches into each data centre. In normal network design aggregation switches come in pairs, the first switch connects over a high speed link to the core switch within the local DC and the second (also over a high speed link) to the core switch in the second DC. All servers are then connected using two separate connections, one to each aggregation switch ensuring that the servers remain present on the network even in the event of a total core switch failure. **The use of Aggregation Switches option is recommended as both a tactical and/ or strategic option**	

3.3.1.3 Costs

The costs associated with options 1 and 2 above are as follows:

Option	Title	Capital	Revenue
1	Do Nothing	£0.00	£0.00
2	Deploy Aggregation Switches at PSHT	£80,142.98	£7,270.00

Total cost for both PSHT and HHCT is below

<u>HHCT CORE</u>

HH comprises a classic 2-layer network build around high speed cores with a single core node located in each of the two data centres for performance and resilience. Each core switch is a [redacted] operating with dual supervisor cards each supporting two switch fabric extensions known as virtual data connections (VDC). Each core switch is fitted with dual power supply modules, both of which are fed from the data centre UPS. The two core switches are joined over dual 10Gb network links that share the core load, providing a 20Gb backbone that forms the core network.

At this time, the two VDC in each switch are split, with one dedicated to user connections and one to server connections. As with PSHT all servers are directly connected to one core switch via the dedicated server VDC available from the [redacted] sited in the DC where the servers are located. There are no aggregation switches in use and none of the servers are dual homed. As a result, a single point of failure exists in terms of server connectivity.

> <u>Risks</u>
> Although the Trust has two core network switches, one in each DC, the use of a single direct connection from servers to the core means that there is a single point of failure should such a connection fail.

3.3.1.4 Options

There are two options open to the Trust with regard to this single point of failure as follows:

1	Do Nothing
The Trust could choose to do nothing and accept the risk. However, this would leave the Trust open to a potentially significant outage should either the link or local core switch fail.	

On this basis the Do Nothing option is rejected	
2	**Deploy Aggregation Switches**
Deploy a number of aggregation switches into each data centre. In normal network design aggregation switches come in pairs, the first switch connects over a high speed link to the core switch within the local DC and the second (also over a high speed link) to the core switch in the second DC. All servers are then connected using two separate connections, one to each aggregation switch ensuring that the servers remain present on the network even in the event of a total core switch failure. **The use of Aggregation Switches option is recommended as both a tactical and/ or strategic option**	

3.3.1.5 Costs

The costs associated with options 1 and 2 above are as follows:

Option	Title	Capital	Revenue
1	Do Nothing	£0.00	£0.00
2	Deploy Aggregation Switches at HHCT	£30,557.52	£3,018.15
	TOTAL Cost for Server Aggregation Switches Trust Wide	**£110,700.50**	**£10,288.15**

PSHT EDGE

As noted above PCH has 34 hub rooms housing one or more edge network switches. This technology comprises a mix of [redacted] switches. The older [redacted] switches reached end of support in November 2015 but are already part of the Trust infrastructure replacement programme. The [redacted] range is current but has an end of support date of October 2019 whilst the [redacted] range, also current, will remain supported until January 2021. Whilst none of the edge network equipment is subject to a maintenance and support contract the Trust holds a range of spare units and parts that is sufficient to sustain the required level of service.

In our opinion the PSHT wired edge network is suitable for continued use as part of a merged Trust.

HHCT EDGE

As noted above HH has 23 hub rooms housing one or more edge network switches. This technology comprises a mix of [redacted] switches from the [redacted] switches have now reached end of support and have been obsolete for some time. As noted above, the older [redacted] switches reached end of support in November 2015, which means that only the [redacted] range are current.

> Risks
>
> At this time only 25% of the total edge network switch technology in the Trust is from a currently supported range. All of the [redacted] switches have already reached end of support [redacted]. Access to replacement hardware components (spares) will also be in very limited supply and given this reliability is also likely to be less than optimum.

3.3.1.6 Options

There are two options open to the Trust with regard to edge network equipment as follows:

1	Do Nothing
The Trust could choose to do nothing and accept the risk. However, as noted above the majority of edge network technology is now fully obsolete and so the risk of failure increases the longer this technology remains in use. The switch software is built on functionality from more than 10 years ago, is not maintained [redacted]. Hardware manufacture ceased some years ago making replacement hardware components (spares) hard to come by. The only option is to commence a rolling programme of replacement as outlined in the HHCT IT Strategy 2014 – 2017. **On this basis the Do Nothing option is rejected**	
2	**Initiate a rolling programme of Edge Switch replacement**
Based upon the age and priority utilisation of the whole edge network, generate and initiate a rolling programme of switch replacement. At this time a total of 75 switches, including new fibre optic modules, is required. Given the scale of this work, this will be categorised as both an immediate task for the most pressing locations (10 Switches across Network Rooms MAN and WPL) and a tactical task for the remaining areas. For optimisation the [redacted] switches have been selected as this is the primary switch in use at PSHT and so, this investment brings the two networks into alignment. **The initiation of a rolling programme of Edge Switch replacement is recommended as both an immediate and tactical option**	

3.3.1.7 Costs

The costs associated with options 1 and 2 above are as follows:

Option	Title	Capital	Revenue
1	Do Nothing	£0.00	£0.00
2	Replace 10 most urgent network switches in Network Rooms MAN & WPL @ £3,794.66 per unit	£37,946.60	See Note 1
	Replace 67 remaining obsolete network switches over a period of 4 years. Review annually as part of Trust merger and plans for the new Health Campus.	£254,242.22	See Note 2
	Total Cost for Edge Switch Replacement	**£292,188.82**	**£0.00**

Note 1: The unit price includes the cost of the switch plus the SPF Fibre modules. There are no associated Professional Services as the Trust IT Department will undertake the decommissioning of old switches and the installation and commissioning of the new units.

Note 2: At this time HHCT holds a small number of legacy switches as maintenance spares. As part of this upgrade two additional switches have been included as services spares rather than engaging in a formal maintenance contract.

3.3.1.8 Recommendations

Immediate: Replace the ten most obsolete edge network switches at HHCT in network rooms MAN and WPL.

Tactical: Over Financial Years 17/18, 18/19, 19/20 and 20/21 replace a further 65 obsolete edge network switches at HHCT, based upon an aged priority plan agreed with IT to mitigate the potential impact of planned/ unplanned down time on IT systems, Telephone and end users across the hospital. Review the plan annually as part of merged Trust requirements and plans for the new Health Campus.

Based upon the Libretti Health review of clinical systems, deploy aggregation switch technology to maximise the availability of both business and clinical systems to meet the organisational needs of the merged Trust.

Strategic: Review developing infrastructure needs at HHCT in-line with Trust IM&T Strategy 2014 – 2017 and direct infrastructure investment as needed, to sustain a modern technology enabled health service.

3.3.2 Wireless Network

🚦	**Immediate**	**Undertake full wireless survey at HHCT**
	Tactical	**Reset or Upgrade wireless network at HHCT based on the outcome of the wireless survey.**
	Strategic	**Continue to invest in network infrastructure as the demand for mobile working will be a major growth area in the merged Trust**

3.3.2.1 Current Position

PSHT

The wireless network at PCH extends across the whole hospital and comprises almost 450 [redacted]. These include AP's from the [redacted] ranges with only the older [redacted] range having an end of support date in July 2018. The wireless network has been installed using the -68dB signal strength making it fit for data, video and voice services over four wireless protocols, these being 802.11a, b, g and n. The Trust also has a smaller wireless network at SRH built to the same standard deployed over 25 [redacted]. Control of the wireless network, as noted above, is managed by [redacted], with one deployed in each of two core network switches. Although technically the standard for Radio Frequency Identification (RFID) is -65dB as this produces a detection accuracy of around 3 metres, the PCH network can provide RFID but with a reduced detection accuracy of around 5 metres.

In our opinion the PSHT wireless network is well designed and suitable for continued use as part of a merged Trust.

HHCT

The wireless network at HH extends across the whole hospital and comprises more than 200 [redacted] These include AP's from [redacted] range with only the [redacted] range having an end of support date in December 2021. It has been installed using the -70dB signal strength which is fit for data and voice services. Control of the wireless network is managed by two [redacted] controllers that are capable of managing up to 1000 AP's and over 12,000 client connections, with one deployed in each of two data centres. Given the -70dB signal strength, it is not possible to operate RFID over the existing HH wireless network.

Risks

Although the HHCT wireless network was designed for both voice and data, IT staff have reported that the delivery of voice services is variable, depending on the location. This is most likely caused by changes to the structure of the hospital and/ or use of the equipment across the hospital.

In our opinion the HHCT wireless network was well designed when first installed but is likely to struggle to deliver voice services in its current state. We would therefore recommend that a wireless network survey is undertaken to confirm what changes are required to resolve service issues. Given that change is going to be required we would suggest that the Trust undertake the survey using the newer -68dB standard (in-line with PSHT) and undertake the change as an upgrade to the HHCT wireless network.

3.3.2.2 Options

There are three options open to the Trust with regard to wireless network equipment as follows:

1	**Do Nothing**
The Trust could choose to do nothing and accept the risk. However, as noted above, video and voice services are key components in a modern digital hospital and highly likely to be required in the merged Trust. **On this basis the Do Nothing option is rejected**	
2	**Undertake wireless survey at -70dB and reset existing network**
The Trust could choose to undertake a wireless survey using the original -70dB and then re-site and add new wireless AP's to reset the network back to its original standard. Whilst this will restore voice as an operable service it would exclude video as the signal strength would remain too low. **This option is acceptable but excludes wireless video going forward**	
3	**Undertake wireless survey at -68dB and upgrade existing network**
The Trust could choose to undertake a wireless survey using the -68dB (in line with the standard used at PSHT) and then re-site and add new wireless AP's to upgrade the network to the higher standard. **This option is recommended as it aligns the two wireless networks**	

3.3.2.3 Costs

Whilst both options 2 and 3 are acceptable each requires a full wireless survey which will result in changes to the network. The resulting work will include moving some of the existing wireless AP's and most likely, adding new ones where gaps are identified. At this time, it is impossible to accurately predict the cost of either option as the amount of work and number of new AP's will not be known until such time as the wireless survey is complete. Therefore, we have allocated a provisional sum of £20,000 to cover the cost of a full wireless survey.

3.3.2.4 Recommendations

Immediate: Undertake a full wireless network survey at HHCT.

Tactical: Based upon the outcome of the wireless network survey, agree network reset or upgrade to ensure wireless meets the services needs of the merged Trust going forward. Factor in the likely needs of the proposed Health Campus as part of the decision making process.

Strategic: Continue to invest in network infrastructure and in particular, the wireless networks as the demand for mobile/ bed side working is already increasing across healthcare and will continue to grow substantially during the next five years.

3.3.3 Network Perimeter

🚦	Immediate	Complete deployment of [redacted]
	Tactical	[redacted]
	Tactical	[redacted]
	Strategic	[redacted]

3.3.3.1 Current Position

PSHT

The PSHT network has a secure perimeter that includes a range of network firewalls, intrusion detection and prevention, e-mail and web filters coupled with other security controls and, an expansive network management platform all overseen by a full time IT Security Officer. At its heart are two primary [redacted], one located in each data centre with each connected to the NHS N3 network. Access to the Internet is provided over the NHS N3 network through the NHS N3 Internet relay. A smaller [redacted] is deployed in the same role at SRH with all three having access to the internet and the secure WAN link that connects the two sites internally (further resilience). All of the network perimeter devices report using a mix of electronic traps (SNMP) and log files to the network management platform which includes an alert module that will immediately notify senior IT staff should a security event occur.

In our opinion the PSHT network perimeter is well designed and suitable for continued use as part of a merged Trust subject to the changes proposed in 3.3.4.

HHCT

The HHCT network has a secure perimeter that includes [redacted], intrusion detection and prevention, e-mail and web filters coupled with other security controls and three local network management platforms. The primary [redacted] units, both located in DC1 and connected to a single core network switch over a single network link. HHCT has two NHS N3 network links with one operating at 50Mb/s and the second at 25Mb/s with each connected to separate primary firewalls. There is also a direct Internet connection that goes out through the secondary firewall in line with the NHS Security Code of Connection. There is a third connection via a secure external zone, known as a DMZ, created as part of the primary firewall configuration. [redacted]

At this time, work is underway to complete the deployment [redacted] and the IT team are receiving assistance from [redacted]

Risks

[redacted]

3.3.3.2 Options

[redacted]

[redacted]

1	Do Nothing
[redacted] On this basis the Do Nothing option is rejected	
2	**Utilise the Aggregation Switches proposed in 3.3.1**
[redacted] This option is acceptable as a short term tactical solution	
3	[redacted]
[redacted] This option is recommended as both a tactical and strategic solution.	

3.3.3.3 Costs

The cost for option 1 is zero and for option 2 is detailed in section 3.3.1.3 above. The cost for option 3 requires a site survey before a price can be reached and so a provisional sum of £25,000 has been included.

3.3.3.4 Recommendations

Immediate: [redacted]

Tactical: [redacted]

[redacted]

Strategic: [redacted]

3.3.4 External Links/ WAN Provision

🚦	**Immediate**	**Consider the early procurement and deployment of a high speed link between PCH and HH.**
	Tactical	**Deploy high speed link between PCH and HH and backup link between SRH and HH using diverse routing.**
	Strategic	**Review links as part of the Trust merger, confirm those to retain, consolidate where possible, add new as required**

3.3.4.1 Current Position

PSHT

The PSHT network has a wide range of external links as shown in the diagram below. These include links to [redacted] for voice services to the NHS N3 network and then onto the Internet, as well as more local links to [redacted] accommodation.

DIAGRAM REMOVED

[redacted] However, it is not envisaged that the remaining links will change, although one or more may be upgraded to provide greater capacity.

HHCT

The HHCT network also has a range of external links, these also include a link to [redacted]

Risks

[redacted]

3.3.4.2 New External Links

As part of the Trust merger there will be a clear need to provide new external links to join the new organisations together. This process will also include additional links to sustain network resilience and, this will likely see a tactical solution emerging early on and then being updated as the new service requirements of the merged organisation become known.

3.3.4.3 Options

The options for links are as follows:

<table>
<tr><th>1</th><th>Do Nothing</th></tr>
<tr><td colspan="2">The Trust merger clearly proposes bringing the two organisations together and in the digital age, this will mandate the provision of external links between the two merging organisations. As a result, there is no option to Do Nothing as without the links the organisations will be unable to work together.
<b>On this basis the Do Nothing option is rejected</b></td></tr>
<tr><th>2</th><th>Create a high speed link between PCH and HH</th></tr>
<tr><td colspan="2">As PCH and HH represent the two main locations for business and clinical activity the ability to pass data, connect voice services, share images and so assure clinical records is key to the Trust operating both an efficient and safe service.
<b>This option is recommended as both a tactical and strategic solution.</b></td></tr>
<tr><th>3</th><th>Create a backup link between SRH and HH</th></tr>
<tr><td colspan="2">As noted above a primary link between PCH and HH is a key requirement for Trust wide service provision. Given this, such a link must be resilient and have a fall-back position should the primary link fail. As SRH is already linked to PCH, classic design would see a third link between SRH and HH complete the loop. This provision also means that any network traffic that has to pass between SRH and HH would have a dedicated link, further improving performance and capacity across the Trust network.
<b>This option is recommended as both a tactical and strategic solution.</b></td></tr>
</table>

3.3.4.4 Costs

The costs associated with options above are as follows:

Option	Title	Capital	Revenue
1	Do Nothing	£0.00	£0.00
2	Provide a high speed 10Gb link between PCH and HH based upon a five-year contract [redacted]	£42,100.00	£30,000.00
3	Provide a backup 1Gb link between HH and SRH based upon a five-year contract [redacted]	£16,800.00	£30,000.00

3.3.4.5 Assumptions

The costs presented above are on the basis that [redacted] are all capable of handling the routing function required for each link. In the event that separate routing equipment is required, cost information for these routers is with the Head of IT.

3.3.4.6 Recommendations

Immediate: Consider the early procurement and deployment of a high speed link between PCH and HH.

Tactical: If not done as an immediate task, procure and deploy a high speed link between PCH and HH as well as a backup link between SRH and HH. Ensure links are, as far as is possible, diversely routed on/ off each hospital campus and in the routes taken between sites.

Strategic: As part of the Trust merger review external links with a view to confirming those that must be retained, consolidate those that provide unnecessary duplication and provide new links to meet the operational requirements of the merged Trust.

3.3.5 Remote Access

🚦	**Immediate**	[redacted]
	Tactical	[redacted]
	Strategic	[redacted]

3.3.5.1 Current Position

PSHT

Remote Access services at PSHT are built around a matrix of the user and device attempting to gain access to the PSHT network as shown in the table below:

DIAGRAM REMOVED

The secure connections into the PSHT network are provided using [redacted] product for Trusted devices and the [redacted]. This approach provides a well-defined and very well controlled means of delivering secure remote access to those users who are authorised to connect from outside.

In our opinion the PSHT approach to Remote Access is exemplary and is very suitable for continued use in the merged Trust.

HHCT

Remote Access services at HHCT [redacted] as is used at PHST to provide a secure virtual private network (VPN) for both Trust Employees and authorised third parties. Trust employees are only able to gain remote access using a Trust device and, HHCT does not permit Trust employees to connect using non Trust or mobile devices (See Note 1). Whilst authorised third parties use the same secure virtual private network (VPN) this is processed through an access list on which the third party must have a registered device. The access list also limits which systems or network services the third party can access. In addition, the access list default setting is closed and so third parties wishing to gain access are only able to do so by making a request via the service desk, at which time an agreed access period is then approved.

Note 1: Whilst the Trust does not provide Remote Access for mobile devices, its adoption of NHSMail2 means that Trust users are able to access their e-mail from outside the Trust over the Internet.

This approach is secure, in particular for authorised 3rd parties, and so safe to continue in the short to medium term. [redacted]

Risks

[redacted]

[redacted]

3.3.5.2 Options

As the number of remote devices that do not attach directly to the HHCT network are few in number and each case is unique, we have chosen not to provide options for review, as we believe that the policy governing remote access should be updated to provide a uniform approach, which is then approved by senior management.

In terms of remote access for mobile devices, HHCT already has a small deployment of a mobile devices management (MDM) package [redacted]. However, this differs from PSHT in that it is a hosted service rather than an on premise solution. In order that future mobile device needs are met, this small scale deployment will need to be considerably expanded.

3.3.5.3 Costs

The costs of expanding the use of the [redacted] comprises the addition of permanent licenses for HHCT which is then offset by the reduction in revenue by moving to on premise as follows:

Title	Capital	Revenue
[redacted]	£15,000.00	£3,300.00
[redacted]	£4,925.00	£1,000.00
[redacted]		-£20,217.60
[redacted]	**£19,925.00**	**-£15,917.60**

3.3.5.4 Recommendations

Immediate: [redacted]

Tactical: As the use of mobile technology is a key enabler for change, develop an approach to remote access at HHCT that facilitates connectivity for authorised mobile devices. Upscale the use of the [redacted] to ensure that NHS encryption and security requirements are met.

Strategic: As part of the Trust merger, review external links with a view to confirming those that must be retained, consolidate those that provide unnecessary duplication and provide new links to meet the operational requirements of the merged Trust.

3.3.6 Management Platform

🚦	Immediate	There are no immediate issues in respect of IT Management Platforms
	Tactical	Resolve network addressing, deploy external links and extend the [redacted]
	Strategic	Develop the use of management platforms, in particular the [redacted] to optimise IT service delivery

3.3.6.1 Current Position

PSHT

There are two management platforms deployed at PSHT, these being [redacted] The [redacted] and management of the wireless network in particular. It is a broad management tool with considerable functionality and sound reporting capabilities[redacted] is a leading third party management platform that is modular in design covering not only networks, but almost all areas of IT Management. It is widely used in health care and across the NHS and is deployed across many areas of IT at PSHT including Digital Communications. The combination of these two management platforms gives PSHT extensive control over not only its Digital Communications but many other areas of IT Service provision. In addition, PSHT has invested in the [redacted], which allows the IT team to set thresholds and traps resulting in electronic alerts should a threshold be exceeded or trap activated.

In our opinion the management platforms deployed by PSHT are suitable for continued use as part of a merged Trust. In addition, we believe that further development of the [redacted] will extend the pro-active approach already adopted by the PSHT IT team and so sustain the high level of IT services as the merged Trust moves forward.

HHCT

There are two management platforms deployed at HHCT, these [redacted] It is a broad management tool with considerable functionality and sound reporting capabilities. The [redacted] is configured to monitor all Trust network equipment through a series of SNMP traps and so will report on any such trap when activated. The combination of these two management platforms gives HHCT adequate control over its Digital Communications.

[redacted]

[redacted]

3.3.6.2 Costs

The costs of extending [redacted]

Title	Capital	Revenue
[redacted]	£12,470.00	£1,248.00
[redacted]	**£12,470.00**	**£1,248.00**

3.3.6.3 Recommendations

Immediate: There are no immediate requirements in respect of the management platform.

Tactical: Once network addressing issues are resolved and the necessary external links are in place between PCH and HH, generate a project plan to deploy the existing [redacted]

Strategic: [redacted]

3.3.7 Presence/ Unified Communications

🚦	**Immediate**	**There are no immediate requirements in respect of Presence or Unified Communications.**
	Tactical	**The Trust should review Unified Communications to improve both business and clinical collaboration**
	Strategic	**The Trust should examine Presence to drive up operational efficiencies and enhance the patient journey**

3.3.7.1 Current Position

Presence

Neither PSHT nor HHCT have much in the way of formal Presence technology at this time. However, the Trust merger OBC was clear in its need for the Trust to adopt more efficient ways of working and to use technology to enable change. Presence is an effective tool that allows hospital staff to locate people, equipment and resources using technology. A classic example of this would be for porters to locate the nearest available wheelchair knowing that it is not in use. This is undertaken by fitting each wheelchair with a unique network tag that would confirm its location on a map of the hospital and whether or not it is occupied. For people this can be done by adding a tag to their Trust ID card or by assigning them a [redacted] as these have Presence built in.

It is recognised that for this to work fully, an upgrade to the Trust wireless network (as outlined in section 3.3.2) would be needed at both hospitals. However, an upgrade at HHCT is already proposed and so developing a business case for Presence in its widest sense, could see considerable savings made, as the efficiencies that it drives deliver potential savings.

Unified Communications

At this time both Trusts have a mixed range of personal communications technology including [redacted], Trust mobile phone, a personal mobile phone and perhaps a mobile tablet device as well. On top of this, access to video conferencing, electronic documents, ward observation systems and one or more personal computers can see busy clinical staff jumping from one technology platform to the next.

Unified Communications (UC) provide the ability to reduce the number of devices required to provide access to existing services as well as providing a platform for future access to information and resources whilst on the move. As with Presence, this is also an area where the adoption of Unified Communications, in particular for busy clinicians, can improve the clinician experience, deliver operational efficiencies and so enhance the patient journey.

PSHT E-Com Project

In respect of Unified Communications, PSHT has already had an initial look at some options for Unified Communications without reaching a final conclusion due to the announcement of a potential Trust merger. What the project did conclude was that there is no one UC product for every staff group, but that the selection of a small number of key UC products, working in harmony, is very capable of delivering the benefits that UC has to offer as outlined above. As a result, it is likely that the Trust would adopt one UC platform for Clinical staff and a variant for business and/ or back office users.

Digital Infrastructure

Both Trusts have the considerable benefit of having the vast majority of their digital infrastructure provided by the same suppliers. This position greatly improves the chances of the Trust reaching sound conclusions without having to worry if what is selected by one organisation, will work at the other following the merger.

3.3.7.2 Recommendations

Immediate: There are no immediate requirements in respect of Presence and Unified Communications

Tactical: As part of the Trust merger and as a means of driving up efficiencies by improving process and enabling change through the use of technology, the Trust should include a further examination of Unified Communications, in particular for clinical staff. Key products to review include [redacted]

Strategic: As part of the Trust merger and as a means of driving up efficiencies by improving process and enabling change through the use of technology, the Trust should examine the use of Presence. It is recognised that one or more upgrades to digital infrastructure are a pre-cursor and so this is set as a Strategic objective.

3.4 Voice Services

3.4.1 Voice over IP (VoIP)

🚦	Immediate	**Procure and install an Analogue PABX at HHCT to provide a fall back solution in the event of a failure of the [redacted] VoIP Telephone System**
	Tactical	[redacted]
	Strategic	**Review the use of both VoIP services as the Trust develops and in particular the proposed Health campus takes shape.**

3.4.1.1 Current Position

PSHT

The delivery of voice over IP is the primary voice service in operation at PSHT. The VoIP solution deployed at PSHT is the [redacted] with two parallel instances, one of which is housed in each DC. This dual instance configuration provides resilience for VoIP users and also facilitates new software testing and system upgrades. Digital Telephone services are delivered to users over the Trust [redacted] utilising both core and edge layers (see section 3.3.1 for further details) and the Trust wireless network (see section 3.3.2 for further details). Voice calls are made and received though a range of desktop handsets that connect to the wired network and walkabout handsets that connect over the wireless network. A directory of VoIP users is maintained within [redacted] and is integrated with Microsoft AD to ensure directory consistency. In the event of a complete collapse of the VoIP system, a reduced telephone service is provided through an analogue PABX (see section 3.4.2 for further details). PSHT also provides a digital voice mail solution using [redacted]

In our opinion the PSHT VoIP solution is robust and resilient, so suitable for continued use in the merged Trust.

HHCT

The delivery of voice over IP is the only voice service in operation at HHCT. It too uses the [redacted]. [redacted]. Unlike PSHT, HHCT do not have an analogue PABX and so are not able to offer a reduced telephone service in the event of a VoIP failure. A directory of VoIP users is maintained within [redacted] and is integrated with Microsoft AD to ensure directory consistency. HHCT also has the same digital voice mail solution as PSHT using the same [redacted]

> Risks
>
> The lack of a second instance or any analogue PABX as a fall-back position is a notable risk to the Trust. As noted above, loss of [redacted] system would result in no landline voice services with only mobile phones ([redacted]) being operable but only where there is a usable signal. In mitigation of this risk a suitable maintenance contract has been placed with [redacted] and who would respond quickly should the [redacted]. However, this would still leave the Trust exposed for a period during which telephone services would be seriously compromised.

3.4.1.2 Options

The options to address the VoIP issues are as follows:

<table>
<tr><th>1</th><th>Do Nothing</th></tr>
<tr><td colspan="2">[redacted]

<b>On this basis the Do Nothing option is rejected</b></td></tr>
<tr><td><b>2</b></td><td><b>Procure and install a</b> [redacted]</td></tr>
<tr><td colspan="2">The Trust could choose to procure and install [redacted]. Whilst use of the spare instance is dependent on the external links, there are two routes planned between HH and PCH (one via SRH).

<b>On this basis this option is not recommended at this time.</b></td></tr>
<tr><td><b>3</b></td><td><b>Procure and install an analogue PABX</b></td></tr>
<tr><td colspan="2">An alternative to deploying a second [redacted] would be to install a small analogue PABX. This would provide a long term fall back solution that could be deployed quickly with the resultant reduction (rather than full mitigation) of the risk. However, the cost of installing an analogue PABX is exacerbated by the need to lay significant copper cabling between the PABX frame room and every network hub room to facilitate hospital wide connection. This will take some time to complete and assumes that every hub room has the capacity to accommodate additional technology. The fall back analogue PABX will include an E1 card, an interface for a single ISDN30 and connectivity for up to 100 extensions over the new copper cable.

<b>This option is recommended as an immediate and tactical solution.</b></td></tr>
<tr><td><b>4</b></td><td><b>Consolidate existing</b> [redacted]</td></tr>
<tr><td colspan="2">As part of the Trust merger process it will be possible to consolidate the [redacted] such that, the Trust reaches a point where three instances are installed in the Trust, with two physically located at PCH and one at HH. Failure of any one should have minimal impact on landline voice services as calls would be re-routed to sustain voice services.

<b>This option is recommended as both a tactical and strategic solution.</b></td></tr>
</table>

3.4.1.3 Costs

The costs of addressing the VoIP issues is as follows:

Title	Capital	Revenue
Do Nothing	£0.00	£0.00
Procure and install a [redacted]	£7,890.00	£1,100
Procure and install an Analogue PABX (estimated cost)	£12,000	£2,400

3.4.1.4 Recommendations

Immediate: Procure and install an Analogue PABX at HHCT to provide a fall back solution in the event of a failure of [redacted].

Tactical: [redacted]

Strategic: Review the use of both VoIP and analogue voice services as the Trust develops and in particular, as the proposed Health campus takes shape.

3.4.2 Analogue Telecommunications

🚦	Immediate	Procure and install an Analogue PABX at HHCT to provide a fall back solution in the event of a [redacted]
	Tactical	[redacted]
	Strategic	Review the future use of analogue telecommunications in particular around the proposed Health Campus development

3.4.2.1 Current Position

PSHT

As noted in 3.4.1 above, PSHT has an analogue telephone system as a fall back to its primary VoIP voice solutions. The analogue PABX includes an E1 card that provides a linked to the [redacted] enabling IP calls to be routed to the analogue extensions during normal operations. These fall back extensions connect to analogue telephones in key locations including wards, clinical departments and senior management offices. In the event of a collapse of [redacted], the E1 card is reconfigured to handle calls over the BT ISDN 30 (link to outside world). Three dedicated extensions have been provided, to which incoming calls are directed and, from which the switchboard operators can transfer calls. The remaining lines on the BT ISDN30 are then available for outgoing calls.

In our opinion analogue telecommunications at PSHT are suitable for continued use in the merged Trust.

HHCT

Again as noted in 3.4.1, HHCT does not have any fall back analogue PABX as all analogue lines are fed through analogue to digital convertors and then processed by the [redacted] instance. [redacted]

The lack of any fall back analogue telecommunications is a significant risk as outlined in 3.4.1 above.

3.4.2.2 Recommendations

Immediate: Procure and install an Analogue PABX at HHCT to [redacted]

Tactical: [redacted]

Strategic: Review the future use of analogue voice services as the Trust develops and in particular, the proposed Health campus takes shape.

3.4.3 Paging

🚦	Immediate	There are no immediate actions required
	Tactical	Test and Deploy [redacted] on mobile phone for those users who work across sites and require paging
	Strategic	Review use of [redacted] as part of Unified Communications Project

3.4.3.1 Current Position

PSHT

As part of the PFI, PSHT has deployed the [redacted] radio paging system right across the Trust. There are six local antenna sites at the [redacted]. The paging platform is managed by the PFI contractor with paging devices being managed by IT. Alongside the [redacted] radio pagers the Trust also has Long Range pagers from [redacted] that need to be kept due to the rural nature of the location. Access to the paging system is through the [redacted] (see section 3.4.4 for further details).

In our opinion the paging systems at PSHT are suitable for continued use in the merged Trust.

HHCT

At HHCT [redacted] is also the radio paging supplier but utilising the newer [redacted] platform. This platform supports the newer pager units as well as a pager application for mobile phones. For radio paging there are two antennas on the roof of separate buildings for resilience. The Trust also has Long Range pagers from [redacted] that need to be kept due to the rural nature of the location. Access to the paging system is via [redacted] on the switchboard which has two separate circuits for resilience.

In our opinion the paging systems at HHCT are suitable for continued use in the merged Trust.

3.4.3.2 Options

As noted above, both pager systems are suitable for continued use in merged Trust and the majority of users will only carry a pager for one site. However, there will clearly be some staff who will work across both sites and as the new clinical services model emerges, this number is likely to increase. In terms of paging services, it will be possible to activate the local paging service via the switchboard from any telephone within the merged Trust. For any user that needs cross site paging, we would recommend the use of the [redacted] paging application on a mobile phone as this provides the optimum service and is also in-line with recommendations around Unified Communications (see section 3.3.7 for further details).

3.4.3.3 Costs

The costs of addressing the Pager issue is as follows:

Title	Capital	Revenue
Total Paging Update Costs	£101,220	£10,000 (est.)

NOTE 1: The paging system at PSHT is provided under the PFI and so the cost information above (which comes directly from [redacted]) does NOT include the PFI uplift and so we believe that the figure should be doubled for budgetary purposes.

3.4.3.4 Recommendations

Immediate: In terms of paging there are no recommendations that require immediate action.

Tactical: Consolidate paging systems such that pages to all users can be initiated from any Trust location. Test and review the use of the [redacted] Paging app for cross site users.

Strategic: Review use of [redacted] Paging App as part of Unified Communications Project.

3.4.4 Switchboard

🚦	**Immediate**	**There are no immediate actions required**
	Tactical	[redacted]
	Tactical	**Consider extending the IVR solution at HHCT to become a Trust wide service.**
	Strategic	[redacted]

3.4.4.1 Current Position

PSHT

The switchboard at PSHT operates through an [redacted] Console System that provides four operator consoles, one supervisor console and one management station; this is augmented by a dual circuit pager console. [redacted]

In our opinion the switchboard at PSHT is suitable for continued use in the merged Trust.

HHCT

The switchboard at HHCT has a total of four telephone consoles plus a further two pager consoles. As noted above, the telephone directory is based upon AD but is augmented by a local spreadsheet that records salient information such as consultant/ secretary relationships. The telephone system is fronted by an Interactive Voice Response (IVR) system that significantly reduces the number of calls handled by the switchboard. However, the IVR platform is very obsolete and needs to be upgraded. There is also a voice link to a local healthnet that includes direct access to local Clinical Commissioning Groups (CCG), Addenbrookes Hospital and many local GP surgeries. The switchboard staff also monitor alarms including cardiac arrest, fire, medical, pharmacy and estates devices, including hospital gases.

In our opinion the switchboard at HHCT is suitable for continued use in the merged Trust.

3.4.4.2 Options

Whilst it is proposed that we consolidate the [redacted] and integrate the paging systems, major technical change to the switchboard is currently unlikely given the monitoring and safety role undertaken. However, as part of the consolidation process, some additional training will be required as operators learn to manage call activity from both sites. Additional resource will also be required to build a new combined electronic directory and to integrate it into the updated switchboard service.

The Trust should also consider extending the IVR deployed at HHCT and this will further automate call handling across the merged Trust and reduce the load on the switchboard service.

As part of the merger process switchboard activity across the two locations should be reviewed as following consolidation, it will be possible to route calls through either switchboard using software.

As a result, the total number of staff on duty at specific times across the working week may be less in a single integrated organisation that in the two current ones.

3.4.4.3 Costs

The costs of extending the IVR service Trust wide is as follows:

Title	Capital	Revenue
Upgrade HHCT IVR Platform to Windows 2012	£21,000.00	£0.00
Procure 4 Virtual Operator licenses for PSHT (see note 1)	£40,000.00	£0.00
Procure 8 Hot Standby licenses	£5,440.00	£0.00
Total Cost of resilient Trust wide IVR solution	**£66,440.00**	**£0.00**

Note 1: PSHT have a new Windows 2012 [redacted] Server installed in August 2016 upon which the virtual operators can run.

3.4.4.4 Recommendations

Immediate: Review the work required to align both IVR systems such that there are consistent messages and options available on 1st April 2017.

Tactical: Consolidate IVR solution such that failure on one site can fall back to the second instance, with the minimum of human interaction. Ensure any fall back is alerted so that appropriate IT staff are notified.

Strategic: Continue to update the IVR as the Trust merger progress in order to optimise the load on switchboard staff.

3.5 Network Addressing

🚦	**Immediate**	**Approach NHS Digital and apply for additional network address numbers within the existing PSHT address range.**
	Tactical	**Identify all existing network numbers in use across the merged Trust. Engage subject matter expertise to support the planning, testing and migration process.**
	Strategic	**Monitor announcements from NHS Digital and the HSCIC in respect of the new HSCN and take action as required.**

3.5.1.1 Current Position

All modern day hospitals use the internationally recognised Transmission Control Protocol (**TCP**) and the Internet Protocol (**IP**) for digital networking. TCP/ IP networks use a numerical network numbering system based upon three classes these being Class A for very large networks, Class B for large networks and Class C for smaller networks.

PSHT

The network at PSHT is a TCP/ IP digital network and uses a portion of [redacted] addresses adopted by the NHS with the exact number ranges being issued to PSHT by NHS Digital.

HHCT

The network at HHCT is also a TCP/ IP digital network but unlike PSHT, uses a [redacted] network address.

3.5.1.2 HSCN Network

NHS Digital (formally The Health and Social Care Information Centre) has already announced the creation of a new Health and Social Care Network (HSCN) as the existing NHS N3 Network contract only to remains in force until April 2020. The new HSCN Network is designed to:

- Establish network arrangements that support the integration of health and social care, regional collaboration and flexible work patterns.
- Establish a marketplace of assured network services that drives competition amongst suppliers, improves consumer choice, supports innovation and delivers value for money.
- Reduce duplication by enabling health and social care organisations to reuse and share existing network infrastructure and services to access the information they need.
- Reduce reliance on a centrally managed, national, private network.

HSCN is designed to support the aspirations set out by the Department of Health and NHS England through the National Information Board – Personalised Care 2020 and NHS England Five Year Forward View. It aims to establish a standards-based approach to network services that will better enable interoperability between health and care organisations and, create a competitive marketplace for the supply and consumption of network services.

These strategies and related national 'pioneer' and 'vanguard' projects cite increased levels of collaboration and integration between health and social care providers as essential to driving improvements and efficiencies. Improved information sharing and the ability to work flexibly to deliver joined up health and social care services to citizens and patients are common features across all these initiatives. It seems almost inconceivable that such ambition could be realised affordably and effectively without providing the underlying standards, infrastructure and services that the HSCN programme will put in place.

Although not known at this time, the provision of HSCN could lead to further changes to NHS Network Addressing, including the possible adoption of IPv6.

3.5.1.3 Options

As part of a merged Trust the optimum operation of the digital network services requires the Trust to operate a single class of network using a range of network addresses from within the same class. However, that is not to say that two networks will not communicate using their existing numbers, but in order to do so, it will be necessary to deploy some routing technology so that resources on the PSHT network know how to reach resources on the HHCT network and vice versa.

It is therefore recommended that such routing technology be deployed and, over time, all network devices currently running on the HHCT network address number range, migrate onto new numbers within the PSHT network number range. In order for this to happen the Trust will need to apply to NHS Digital for additional numbers within the PSHT range, to be allocated to the Trust.

Once done, engage subject matter expertise and generate a detailed plan for network address migration on a stage by stage basis. Agree where numbers or groups of numbers can be migrated using automation (i.e. DHCP ranges) and what will need to be moved manually. Test migration at each stage before executing the next. Work with suppliers and external 3rd parties (i.e [redacted]) to ensure that changes in network address do not result in a loss of connectivity. Ensure that external services such as Remote Access and Web services continue to work as expected throughout the migration. Maintain a fall-back position for each stage of the plan.

3.5.1.4 Costs

There are no infrastructure costs to amend the network addressing schema other than additional resource, details of which are included in section 3.14 on Professional Services.

3.5.1.5 Recommendations

Immediate: Approach NHS Digital and apply for additional network address numbers within the existing PSHT network address range.

Tactical: Identify all existing network numbers in use across the merged Trust. Engage subject matter expertise to support the planning, testing and migration process.

Strategic: Monitor announcements from NHS Digital in respect of the new HSCN and take action as required.

3.6 Computing Devices

Immediate	There are no immediate actions required for computing devices
Tactical	Identify failing or fault-prone Desktop and Laptop PCs from Service Desk reports and replace as soon as possible. Initiate major PC rollout programme at HHCT.
Strategic	Continue the rolling programme of PC replacement based on age, reliability, functionality, and upgradability.

3.6.1 Desktop/ Laptop

3.6.1.1 Current Position

PSHT

There are approximately 3,000 Desktop and Laptop PCs in use, the vast majority having been updated to Windows 7. There are still a few PCs and items of medical equipment with embedded PCs that cannot be upgraded due to equipment suppliers not supporting up-to-date operating systems. The risks around these are being managed by the IT teams and user departments.

As part of the PSHT annual IT budget, a sum of £167,000 is provided to replace workstations and supporting peripherals that have reached end of life. This is important as it allows the IT department to identify equipment that fails repeatedly (via the service desk) and those that make up the oldest tranche still in use, and schedule these for replacement.

HHCT

There are approximately 1,900 Desktop and Laptop PCs in use, the vast majority having been updated to Windows 7. There are still a few PCs and items of medical equipment with embedded PCs that cannot be upgraded due to equipment suppliers not supporting up-to-date operating systems. The risks around these are being managed by the IT teams and user departments.

Identified in the HHCT IT Strategy is a priority need for a rolling replacement of aging workstations with the aim that there should be no operational workstations that exceed four years of age. The strategy sets out a time line and an approach, however, due to funding constraints, only around 400 new workstations have been deployed over the past three years.

3.6.1.2 Options

The options to address this issue are as follows:

<table>
<tr><td><b>1</b></td><td><b>Do Nothing</b></td></tr>
<tr><td colspan="2">The Trust could choose to take no action and continue to let the personal computer estate continue to age. It is a high risk strategy as the longer the estate is left the greater the risk of failure or incompatibility becomes. As this was identified as a Strategic aim in 2014 and little has been done to date, some workstations at HHCT are now approaching 8 years of age and so this issue must be addressed.

<b>On this basis the Do Nothing option is rejected</b></td></tr>
<tr><td><b>2</b></td><td><b>Utilise the existing budget only for replacement</b></td></tr>
<tr><td colspan="2">As part of the Trust merger the total number of workstations will exceed 3500 with a notable disparity between those at PSHT and those at HHCT. At present the current budget allows for a maximum of 400</td></tr>
</table>

new units per annum, however with the increase in workstation number this would see the replacement cycle set at 8 years.

On this basis this option is also rejected

3 Increase the existing budget to £300,000

As part of the Trust merger, technology will be a key enabler supporting change. The proposed increase in budget is proportional to the scale of additional workstations but does not take account of the impact of an already ageing estate at HHCT. As a result, it will take 5 years to reach parity during which the risk of failure and/ or incompatibility is reduced but not mitigated.

This option should only be considered as a position of last resort

4 Invest a capital sum and increase the existing budget to £300,000

In recognition of the key role technology has to play in enabling change and the aging estate of workstations at HHCT, the Trust could choose to invest a capital sum (estimated to be around £320,00) to replace all workstations over four years of age and increase the IT replacement budget to £300,000 per annum. This option would see the merged Trust move forward to a six-year cycle for workstations including a mid-point upgrade to memory and solid state disks where appropriate.

This option is recommended as the optimum tactical solution.

5 Virtualise the desktop

An increasing number of organisations globally, are seeking to virtualise the desktop. Whilst this does not completely remove the need for workstations it does significantly reduce the number. In the place of a workstation a virtual terminal is deployed at a lower unit cost and with a longer life cycle. This virtual terminal allows a user to login after which his/ her virtual desktop is downloaded to the virtual terminal. Whilst there are many benefits in the longer term, there is also a need to make moderate investment in technology in the data centre up front to deliver the virtual desktop infrastructure (VDI).

On this basis this option is recommended only as a strategic solution.

3.6.1.3 Costs

The costs of addressing the Desktop/ Laptop issues are as follows:

Title	Capital	Revenue
Do Nothing	£0.00	£0.00
Utilise existing budget for replacement	£0.00	£167,000.00
Increase existing budget to £300k	£0.00	£300,000.00
Invest Capital and increase existing budget to £300k	£320,000.00	£300,000.00
Virtualise the Desktop	See Note 1	

Note 1: Whist it would have been possible to generate an estimated cost for a VDI, the greatest benefit is when VDI is combined with mobility for Clinical Applications. This gives Clinicians the ability to access patient data on the move almost regardless of the device they are using. To reach a price with any meaning, it is necessary to know which clinical systems need to be included. At this time work is being undertaken by Libretti Health around the consolidation of Clinical Applications for the merged Trust and until this is complete it is not possible to generate a cost.

3.6.2 Mobile Phones and Tablets

3.6.2.1 Current Position

PSHT
There are approximately 600 tablets in use, mainly iPads and iPods and some 270 phones.

HHCT
There are approximately 400 tablets in use, mainly iPads and some 200 phones.

3.6.3 Security Suite

3.6.3.1 Current Position

PSHT
PSHT have deployed [redacted] to provide protection for all its computing devices. It is an advanced agent based solution that operates on all forms of workstation, file servers and mobile devices. The agent software includes encryption, e-mail security and a range of Internet protection tools. It is managed through a central management console and can be fine-tuned to better meet the cyber security needs of the Trust.

HHCT
HHCT utilises [redacted] which covers all of its workstations and file servers. It is an advanced agent based solution providing encryption, anti-virus and malware protection, desktop host intrusion and firewall, web security and e-mail security all of which is delivered through a single management console.

3.6.3.2 Options

Each of the Security Suite products are advanced technical solutions and each provides a high level of device protection. However, the scope of the [redacted] is wider, including protection for mobile devices and this combined with the granular nature of the agent which permit fine tuning means that we believe this to be the better solution for the merged Trust.

3.6.3.3 Costs

Title	Capital	Revenue
[redacted] across the merged Trust (see Note 1)	£30,000.00	£0.00

The [redacted] for PSHT is based upon a 2-year deal paid for from Capital.

3.6.4 Recommendations

Infrastructure requires constant review and rolling systems of upgrade/ replacement in order to support existing and new services and applications. As such, an annual budget for this rolling replacement is required to avoid unnecessary downtime due to device failure. Given the base number of almost 5,000 units in the merged Trust and a replacement cost of approximately £400 each, it is suggested that 20% are replaced annually at a cost of £400,000 per annum.

Immediate: No immediate actions required.

Tactical: Identify failing or fault-prone Desktop and Laptop PCs from Service Desk reports and replace as soon as possible. Initiate major PC rollout programme at HHCT.

Strategic: Continue the rolling programme of PC replacement based on age, reliability, functionality, and upgradability.

3.6.5 Single Sign-on

3.6.5.1 Current Position

PSHT have some 500 single sign on licenses and for clinical staff in particular, the advantages are clear. One login, entered once and then secure access to all systems for which authorised access has been provided. However, the primary benefit lies in the fast access to clinical systems avoiding the need to login/ logout every time access to patient information is needed. Yet in parallel with this Infrastructure review, the Trust has also commissioned a review of its clinical systems. As part of this, it is understood that PSHT needs to introduce a new Patient Administration System (PAS) quickly and so these items combined will lead to a delay in the start to any single sign on project. Once the choice of systems to go forward is known, the Trust should then be able to move forward quickly.

3.6.5.2 Costs

Below are the costs for single sign on for the merged Trust:

Title	Capital	Revenue
Single Sign on appliances and software	Unknown at time of issue	Unknown at time of issue

3.6.6 Recommendations

As noted above, the use of single sign produces many benefits, in particular for clinical staff, in terms of speed of access, no repeated ID and password entry and when combined with context the ability to take a single patient ID across multiple systems. We would therefore recommend as follows:

Immediate: No immediate actions required.

Tactical: Monitor the progress of clinical systems consolidation and as key systems are merged and come on line, commence testing single sign on for live use. Once critical mass is reached, rollout single sign on for clinical users.

Strategic: Continue to ascertain where single sign on be beneficial, consider using for mobile computing and multi-system non clinical users.

3.7 Compute and Storage

🚦	**Immediate**	**Upgrade the existing SAN and procure a send instance. Establish data replication to facilitate fast recovery and sustain data backup.**
	Tactical	**Implement Disk to Disk to Tape Backup process at Hinchingbrooke with Disk and Tape backup devices housed in the empty DC1 (see section 3.2.1)**
	Strategic	**In light of clinical system review establish funding for a rolling replacement programme of servers and storage devices based on age/warranty/reliability.**

3.7.1 Current Position

PSHT

The server base of 100 machines is mainly Dell with a small number of non-Dell machines used for managed services.

Administration Tools

[redacted]

Monitoring

[redacted]

SQL

[redacted]

VM

[redacted]

[redacted]

Storage

[redacted]

[redacted]

[redacted]

[redacted]

3.7.1.1 Options – PSHT Compute

The options to address this issue are as follows:

1	Do Nothing
The Trust could choose to take no action but this would impact the current programme and/ or delay the progress of the merged Trust. Whilst the compute platform at PSHT is sufficient for the current workload, there is limited head room to grow and work is already planned that will utilise the head room that is left. **On this basis the Do Nothing option is rejected**	
2	**Provide additional compute**
The Trust may choose to provide additional compute capacity to ensure that PSHT has sufficient performance, capacity and headroom to meet the needs of the merged Trust. **This option is recommended as a tactical solution.**	

3.7.1.2 Costs – PSHT Compute

The costs of addressing the PSHT compute requirements are as follows:

Title	Capital	Revenue
Do Nothing	£0.00	£0.00
Provide new ESXi Compute platform	£55,236.21	£5,590.17
Total cost for recommended option	**£55,236.21**	**£5,590.17**

3.7.1.3 Options – PSHT Storage

The options to address this issue are as follows:

1	Do Nothing
The Trust could choose to take no action but this would impact the current programme and/ or delay the progress of the merged Trust. As of today there is sufficient storage to meet the Trust needs but not those of the merged Trust. **On this basis the Do Nothing option is rejected**	
2	**Upgrade the SAN at PSHT**
The Trust may choose to upgrade the SAN at PSHT as this would provide the additional storage required to support the merged Trust. **On this basis this option is recommended**	

3.7.1.4 Costs – PSHT Storage

The costs of addressing the PSHT SAN requirements are as follows:

Title	Capital	Revenue
Do Nothing	£0.00	£0.00
Upgrade SAN	£56,187.57	£6,019.27
Total cost for recommended option	**£56,187.57**	**£6,019.27**

HHCT

The server base of 70 machines is mainly HP with a small number of non-HP machines used for third party services.

Servers

[redacted]

DIAGRAM REMOVED

[redacted]

3.7.1.5 Storage

[redacted]

3.7.1.6 VM

[redacted]

3.7.1.7 Backup and Maintenance

[redacted]

3.7.1.8 Options – SQL Server – Trust Wide

The options to address this issue are as follows:

1	Do Nothing
The Trust could choose to take no action but this would leave the primary database technology at risk, in particular at HHCT. At this time many of the instances of SQL Server at HHCT are obsolete [redacted]	

On this basis the Do Nothing option is rejected	
2	**Provide additional compute**

The Trust may choose to upgrade its SQL Server Cluster to the newer 2012 release which is still supported by Microsoft, is known to work with the business and clinical databases in use at the Trust thereby removing the risk.

This option is recommended as a tactical solution.

3.7.1.9 Costs – SQL Server

The costs of addressing the HHCT compute requirements are as follows:

Title	Capital	Revenue
Do Nothing	£0.00	£0.00
Upgrade SQL Cluster to SQL Server 2012	****	£162,000
Total cost for recommended option	****	**£162,000**

3.7.1.10 Options - Compute

The options to address this issue are as follows:

1	Do Nothing

The Trust could choose to take no action but this would leave the primary compute function at risk. At this time there is barely sufficient processing capacity with very little head room for growth. In addition, some elements of the compute are already legacy in terms of age and function.

On this basis the Do Nothing option is rejected

2	Provide additional compute

The Trust may choose to provide additional compute capacity to ensure that HHCT has sufficient performance, capacity and headroom to meet the needs of the merged Trust.

This option is recommended as a tactical solution.

3.7.1.11 Costs - Compute

The costs of addressing the HHCT compute requirements are as follows:

Title	Capital	Revenue
Do Nothing	£0.00	£0.00
Provide new ESXi Compute platform	£55,236.21	£5,590.17
Total cost for recommended option	**£55,236.21**	**£5,590.17**

3.7.1.12 Options - Storage

The options to address this issue are as follows:

1	Do Nothing

The Trust could choose to take no action but this would leave the primary compute and storage function at risk. There is insufficient storage, in particular at HHCT, to meet the needs of the merged Trust and part of this is already legacy in terms of age and function.

On this basis the Do Nothing option is rejected

2	Upgrade single SAN at HHCT

The Trust may choose to only upgrade the single SAN at HHCT. This would provide the additional storage required to support the merged Trust but the data would not be replicated meaning any failure would require a manual restore with many hours of system down time. **On this basis this option is also rejected**	
3	**Upgrade single SAN at HHCT and provide second instance**
The Trust may choose to not only upgrade the single SAN at HHCT but also to provide a second instance. This would provide the additional storage required to support the merged Trust and the data would be replicated onto the second SAN allowing IT to immediately recover any lost data with either minimal or no system down time. **This option is recommended as an immediate and tactical solution.**	

3.7.1.13 Costs

The costs of addressing the HHCT SAN requirements are as follows:

Title	Capital	Revenue
Do Nothing	£0.00	£0.00
Upgrade single SAN	£28,174.73	£3,110.17
Upgrade single SAN and provide 2nd Instance	£324,432.38	£29,197.23
Total cost for recommended option	**£324,432.38**	**£29,197.23**
4 Node SAN Uplift (See consideration below)	**£30,000.00**	**£2,716.00**

3.7.1.14 Consideration

Whilst the sections above address the storage needs of PSHT and HHCT the result will be a two node SAN at PSHT and a two node SAN at HHCT. The proposed changes could go further by using the opportunity to build a single four node SAN that covers both sites. The advantage of the four node SAN is twofold: firstly, the technology used would provide additional headroom allowing storage growth by only adding more disks and shelves (as opposed to the more expensive enclosures with fibre channel links). Secondly, the management platform would see it as a single source making management tasks (including data replication, data movements between tiers – even across campus) easier and greatly more visible. The cost of the uplift to a four node SAN is shown above.

3.7.1.15 Recommendations

Immediate: Upgrade the existing SAN and commission a second instance. Establish data replication to facilitate fast recovery and sustain data backup.

Tactical: Implement Disk to Disk to Tape Backup process at Hinchingbrooke with Disk and Tape backup devices housed in the empty DC1 (see section 3.2.1)

Strategic: In light of clinical system review establish funding for a rolling replacement programme of servers and storage devices based on age/ warranty/ reliability.

3.8 Service Desk

🚦	Immediate	Recruit to fill existing vacancies in Service Desk teams
	Tactical	[redacted] Service Desk software Hinchingbrooke, retain on-site teams at each location
	Strategic	Align Service Desk capacity with requirements of the merged Trust's service offerings

The Service Desk teams at Peterborough and Hinchingbrooke have experienced, knowledgeable and diligent people within them who achieve remarkably high User Satisfaction scores in regular surveys. They are to be congratulated and valued for their work. The detailed review findings are listed below followed by our conclusions.

3.8.1 Peterborough – Current Situation

3.8.1.1 Tools and Resources

- The Service Desk at Peterborough is led by [redacted]
- The Service Desk provides a non-technical call logging service, along with password resets and basic advice
- Calls are passed to technical support teams for infrastructure support, and to the Informatics and Training Support team for application specific training and support. Access to applications is managed through the Security Access Manager (SAM)
- SAM is built on the [redacted] functionality and provides a mechanism for users to request access to applications and functions with a detailed audit trail of requestors and approvers
- A third line technical team carry out infrastructure monitoring and provide in depth technical backup for the other Infrastructure support teams
- The teams use [redacted] for call-logging, process support, monitoring, alerts and reporting. There is also a self-service portal on [redacted] currently used for approximately 65% of all incidents
- [redacted]
- The IT Service Catalogue data/ queries held within the Service Desk details current services provided by the IT department along with applications which are supported.

[redacted]

[redacted]

- Discovery and Inventory of networked assets
- Software license management
- Operating software provisioning and migration based upon template-driven processes to deploy operating systems using hardware-independent imaging, driver management, and integrated software delivery
- Software Distribution and Packing allowing IT to distribute software across the Trust to multiple platforms and devices in minutes using minimal infrastructure and network traffic. It can also be used or provide an app store experience for self-service app deployments

- Alerting and Monitoring - allowing alerts to be set for end user devices and/ or servers either singularly or as part of a more complex workflow
- Remote Control allowing technical staff to take over the remote machine and quickly remedy the reported fault
- Dashboards and Reporting - providing senior management with dashboards on their mobile devices and detailed reports to improve IT decision-making.

[redacted] Suite is a high valuable addition to the base [redacted] application and is key to the management of computing devices.

3.8.1.3 User base

- There are approximately 7,500 users, 5,500 of which come through the ESR interface. Others include students, trainees, visiting consultants etc.
- There are around 3,000 PCs on the system plus 600 tablets including iPads and iPods
- Also on the inventory are 270 active phones and some non-Microsoft software

3.8.1.4 Training

- One-to-one training given on induction and some Customer Services courses planned
- [redacted] administration course scheduled for October

3.8.1.5 Prioritisation

- Calls are assigned a Priority level based on a matrix of Severity and Criticality. These criteria are defined as follows:

  Criticality

  Each Specific Service Description listed in the IT Service Catalogue is defined (and agreed with Trust Management) as falling into one of the following three groups of 'Service/ System importance' or Criticality which are:

  - Critical
  - Important
  - Complimentary

  These 3 levels are defined by the effect that their ***complete prolonged unavailability*** would have on the Trust's business.

  Critical

  Core business functions would cease to function effectively with a detrimental impact on:

  - safety
  - patient care
  - finances
  - the Trust's reputation

  Important

  A severe impact on the patient experience or functioning of the Trust or department, but would not stop the Trust from carrying out its core business.

Complimentary

System used departmentally that would only have impact in one area of the organisation; or systems used Trust-wide to compliment the running of the organisation. Includes end-user developed or commissioned applications about which the I.T. department has very limited knowledge or expertise.

N.B. It should be noted that whilst some systems are very important to their departmental or Trust-wide users, they might not severely impact the core business of patient care.

Severity

Five levels of Incident Severity are defined. These are determined by the nature of the incident, the potential consequences of the incident and numbers of people affected:

Severity 1

Immediate threat to safety or systems security
Complete unavailability of critical service/ system

Severity 2

Serious impact on patient experience
Partial unavailability of service
Partial loss (or serious degradation of) the functionality of a system

Severity 3

Moderate impact on patient experience
System/ service functionality/ performance is degraded such that effectiveness of a group of users is reduced
Complete loss of individual access to or use of a system or service.

Severity 4

System/ service functionality/ performance is degraded such that effectiveness of a single user is reduced
Inconvenience to multiple users

Severity 5

Inconvenience to single user
'How do I' type queries

The matrix defines the Priority level assigned.

	1 - Critical	2 - Important	3 - Complimentary
Severity 1	P1	P2	P3
Severity 2	P2	P3	P4
Severity 3	P3	P3	P4
Severity 4	P4	P4	P5
Severity 5	P5	P5	P5

- The [redacted] software contains built-in alerts for monitoring and escalating an incident based on its Priority rating

3.8.1.6 Monitoring and Reporting

- The teams monitor the progress of incident resolution using the functions of the [redacted] program to provide automatic alerts at each stage of the process
- Monthly reports are created and published at the start of each month. Query data is exported allowing the Service Desk to create seven spreadsheets in total, with multiple charts per spreadsheet:
    - Incident by Asset (x1)
    - Used to identify rogue PC's or printers. Used by Infrastructure Support Manager and Senior Analysts

    - Incidents by source (x2)
    - Reporting on source breakdown, showing gradual increase of Self-Service and SAM (Service Catalogue) calls. Both for the previous month and trend over time. Used by Infrastructure Support Manager/ Team Leader to drive move towards Self Service.

    - Incidents by time to resolve (x3)
    - Broken down by support team (drill down available to individual analyst) and by call priority. Breaches by team. Used by team managers to monitor performance, work load sharing etc.

    - Incidents by response time (x1)
    - Detailing proportion of calls by priority vs response time targets as per SLA document (see point 3 above). This was produced at Jon Peate's request. It is a contractual deliverable for the Pathology department to support their certification.
- The above are published by emailing a shortcut primarily to the IT Managers. A subset of information is sent to Health Records (EDM – Electronic Document Management), Data Quality, and ERostering managers also by email.
- [redacted] reports on PC Virus calls stats and incidents logged relating to Security. These are simple list in format and go to the Head of IT and the IT Security Advisor.
- Real time dashboards are used to show outstanding call volumes by team and site and warning of calls to breach within the next 4 hours. The performance dashboard also shows calls logged and resolved that day. Three dashboards in all are used by the Infrastructure Support Manager to monitor daily workload.
- [redacted] has a forthcoming add-on called "Extraction" which could enhance and simplify the data extraction and reporting process.

3.8.1.7 Reviewing

- Queries and comments on the monthly reports issued to IT Managers are regularly received and there is regular discussion within the Service Desk about incidents from which they can learn.
- Knowledge sharing within the team is ongoing and actively encouraged.

3.8.1.8 Escalation

- There is a well-defined escalation process documented in the SLA mentioned earlier. Breaches are closely watched to understand why the breach occurred and examine what could have been done if anything, to prevent it.

3.8.1.9 Change Management

- The I.T. Department operates a Change Management process on behalf of the Trust. If any support incident results in a "Change", the person managing the incident will submit the change to the *Change Manager* (I.T. Infrastructure Service Manager) for consideration by the *Change Advisory Panel* (CAP).
- There are different classes of change, including "standard" and Emergency" to cope with different support scenarios. Any decision by the CAP which would expose the Trust to a risk graded as *Significant* or *High* will be reviewed by the Head of I.T.

3.8.1.10 Problem Management

- A Problem Management process is defined within [redacted]. The process is new and will be used adhoc, when a specific issue is identified which requires special focus. (An example in the past was 'slow logon') The Problem Management process provides a framework to identify, investigate and test possible root causes, until the problem is deemed to be brought under control.
- The Problem Management team is similar in structure and membership to the Change Management team, and is also lead by the I.T. Infrastructure Support Manager.

3.8.1.11 Stock Control

- The Service Desk team maintain the recommended hardware options published on the IT department website.
- Users raise orders for items described on the website directly with Purchasing and Supplies (P&S); P&S email the Service Desk for authorisation before placing any IT order. This allows them to ensure that what is being ordered is either 'standard' equipment, or if non-standard, can be assessed for compatibility before an order is placed.
- At the time an order is 'authorised', it is recorded on Service Desk enabling it to be tracked.
- The Service Desk record is updated on delivery, at which time the equipment will normally be added to the inventory, before a member of the support team delivers it to the user and undertakes the install.

3.8.1.12 Challenges

- Should the merger be approved, there will be challenges surrounding Active Directory; the optimum would be to create a new AD and transfer existing records on a planned basis. The Inventory could probably be imported to the new AD quite easily with work done on the Location field. User records could be imported but would require de-duplication across the sites.
- Servicing of external clients (CCGs etc.) would ideally be achieved by extending [redacted] to them; this requires further investigation.

3.8.2 Hinchingbrooke Current Situation

3.8.2.1 Tools and Resources

- The Service Desk at Hinchingbrooke is led by [redacted]
- The Service Desk team use [redacted] software for logging, managing and reporting calls to the Help Desk, this is run on a hosted Cloud platform.

- The hours covered are 8am – 5pm Monday - Friday using 4 junior operators and 2 Technical operators, although one of the Technical operator position is vacant at present. Out of Hours cover is provided for emergencies only but is often abused.
- In addition, Danwood support the Managed Print service

3.8.2.2 Asset Management

Alongside [redacted] management application. The [redacted] application is able to identify and record any new device when it joins the network. If the device uses recognised operating software, such as Windows, [redacted] is then able to take an inventory of all the software loaded on the device including any software serial numbers. These are then matched against an internal database to provide a human readable list of software held against the device.

3.8.2.3 User Base

- [redacted] As well as supporting HHCT (1,900 users), the Team also provide desktop support to CCG GP Sites, Cambridge Community Services and Cambridge Mental Health Trust (1,000 users), a total of approximately [redacted]
- The number of calls varies between 75 - 130 per day.

3.8.2.4 Training

- There is almost no formal training due to budgetary constraints. Staff are trained 'on the job' by their colleagues.

3.8.2.5 Prioritisation

- There are four levels of priority: Low, Normal, High and Urgent. All calls are logged as Low initially, Normal and Urgent are hardly used, High is used when the user states that the issue is a high impact problem or when the senior team members view it as high impact.

3.8.2.6 Service Levels

- There is no formal Service Level Agreement in place.

3.8.2.7 Monitoring

- Senior Desktop Agent monitors activity and [redacted] provides alerts based on priority and time, e.g. email alert if the call has not been updated in 5 days.
- [redacted] provide regular reports of Help Desk activity including notifying the IT Operations Manager [redacted], of any issues ongoing for more than 90 days.

3.8.2.8 Reviewing

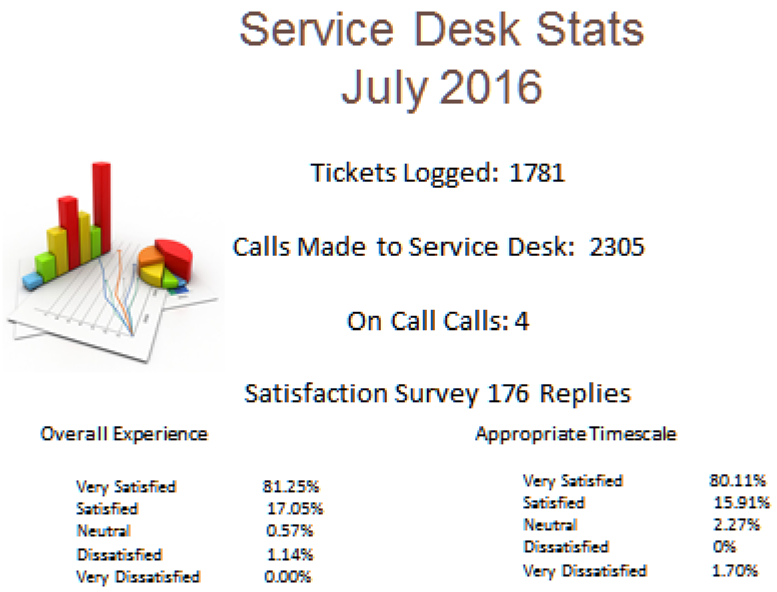
- A fortnightly review of calls reported is discussed at the Operations team meeting.

3.8.2.9 Change Management

- All changes are assessed by the Change Board, which has Operations and Clinical representation. The process operates well with the exception of some changes introduced by third-party software suppliers which have been agreed with the clinicians, but not always notified to Operations.

3.8.2.10 User Satisfaction

- User satisfaction is very high as shown in the report for July 2016 illustrated below.
- Zendesk sends an automated email following closure of an incident where the user is asked to rate the service they received; an example of the report on user satisfaction is shown below:



Service Desk Stats
July 2016

Tickets Logged: 1781

Calls Made to Service Desk: 2305

On Call Calls: 4

Satisfaction Survey 176 Replies

Overall Experience		Appropriate Timescale	
Very Satisfied	81.25%	Very Satisfied	80.11%
Satisfied	17.05%	Satisfied	15.91%
Neutral	0.57%	Neutral	2.27%
Dissatisfied	1.14%	Dissatisfied	0%
Very Dissatisfied	0.00%	Very Dissatisfied	1.70%

3.8.2.11 Team Spirit

- Adam is a very positive leader and his team are usually animated, sharing and positive about the work they do.
- The potential merger is seen as an opportunity to strengthen the Help Desk team with knowledge-sharing and extended hours.

3.8.2.12 Challenges

- Should the merger proceed, the challenges will be taking advantage of the combined pool of Help Desk resources to achieve both knowledge sharing and maintain an on-site presence.

3.8.3 Options

In considering the Service Desk options, the issue are as follows:

1	**Do Nothing**
The Trust could choose to take no action but this would leave each hospital running its own local Service Desk solution without any visibility of service desk call and incidents across the merged Trust. **On this basis the Do Nothing option is rejected**	
2	**Deploy [redacted] Trust Wide**
The Trust may choose to replace the HHCT Service desk by extending the PSHT [redacted] Service Desk [redacted]) to become a Trust wide solution. This option would then provide users, regardless of location, the ability to log calls into a single service desk. It would also allow technical staff to share their experience when resolving faults as well as building single links to all third party support services	

including any relevant external Service Level Agreements. This option would also see a small revenue savings from the cessation of [redacted] **On this basis this option is a sound tactical and strategic solution**	
3	**Deploy [redacted] and the Management Suite Trust wide.**
The Trust may choose to not only deploy the [redacted] Trust wide by also to extend the use of the [redacted] across the whole merged Trust. Many of the tools including in LDMS support fault resolution, save considerable time or provide alerts and warnings, often a part of a complex workflow. These are invaluable to the service desk in delivering a high quality service which is reflected in the satisfactions scores achieved. This option would see [redacted] **This option is recommended as an immediate and tactical solution.**	

3.8.4 Costs

The cost of addressing the Service Desk issues are as follows:

Option	Title	Capital	Revenue
1	Do Nothing	£0.00	£0.00
2	[redacted]	£5,250.00	£1,000.00
	[redacted]	£0.00	£14,100.00
3	[redacted]	£5,250.00	£1,000.00
	[redacted]	£0.00	£14,100.00
	[redacted]	£51,250.00	£9,250.00
	[redacted]	**£56,500.00**	**£24,350.00**
	[redacted]	£0.00	-£8,814.28
	[redacted]	£0.00	-£18,600.00
	Total cost for recommended option	**£56,500.00**	**-£4,064.28**

3.8.5 Service Desk Recommendations

The levels of staffing of the Service Desk at each location are cost-effective and excellent value-for-money especially when viewing the high user satisfaction results. During the merger there will be increased problem/ incident activity as a consequence of change even though that change will be very well planned. It is therefore recommended that vacancies on the Service Desk teams are filled prior to merger activity to allow time for staff training. The performance of the Service Desk teams during merger activity will have a strong impact on the success of changes and the perception of the quality of the merger process by all users; it is therefore important to resource and support these teams in the critical role which they will play.

In light of this, the recommended option is that the [redacted] software including the Management Suite with its attendant processes, is implemented at Hinchingbrooke so that a complete view of activity can be monitored and reported across the merged Trust. In taking this option the Trust will also generate a small revenue saving from a highly upgraded and now fully integrated Service Desk across the merged Trust.

3.9 Active Directory

🚦	**Immediate**	**Split the Flexible Single Master Operation roles across the DCs at Hinchingbrooke with the PDC emulator going on the server with the lightest load**
	Tactical	**Set up a transitive forest trust relationship between the Peterborough and Hinchingbrooke instances of Active Directory. This will allow resources on one domain to be made available to the other and vice-versa.**
	Strategic	**Define a single schema, two-tree, two-domain, single forest for the merged NHS Trusts. Migrate the existing AD domains to the new forest over time.**

Both sites have a very straightforward Active Directory with single forest, single tree and single domain structures. This makes for easier maintenance and support.

3.9.1 Peterborough - Current Situation

The AD topology shows:

DIAGRAM REMOVED

The topology shows an efficient spread of the Flexible Single Master Operation roles (FSMOs) with the PDC emulator being on a separate DC. Amongst other things, the PDC Master acts as the final authority on password authentication and needs to be immediately available for password changes and arbitration. The Infrastructure Master is not used in a single domain environment so its placement is irrelevant in this scenario. Microsoft recommend that the Schema Master and Domain Naming Master, both lightly used, are held on the same DC. Finally, the RID Master is used to supply Relative IDs to the Domain Controllers; it does so in blocks so immediate response is not critical except when adding large numbers of new users.

3.9.2 Hinchingbrooke – Current Situation

The AD topology shows:

DIAGRAM REMOVED

At Hinchingbrooke, all the FSMOs are held on the one Domain Controller which can become a bottleneck on larger domains with high levels of change activity.

3.9.3 Recommendations

Immediate: Split the Flexible Single Master Operation roles across the DCs at Hinchingbrooke with the PDC emulator going on the server with the lightest load.

Tactical: Set up a transitive forest trust relationship between the Peterborough and Hinchingbrooke instances of Active Directory. This will allow resources on one domain to be made available to the other and vice-versa.

Strategic: Define a single schema, two-tree, two-domain, single forest for the merged NHS Trusts. Migrate the existing AD domains to the new forest over time.

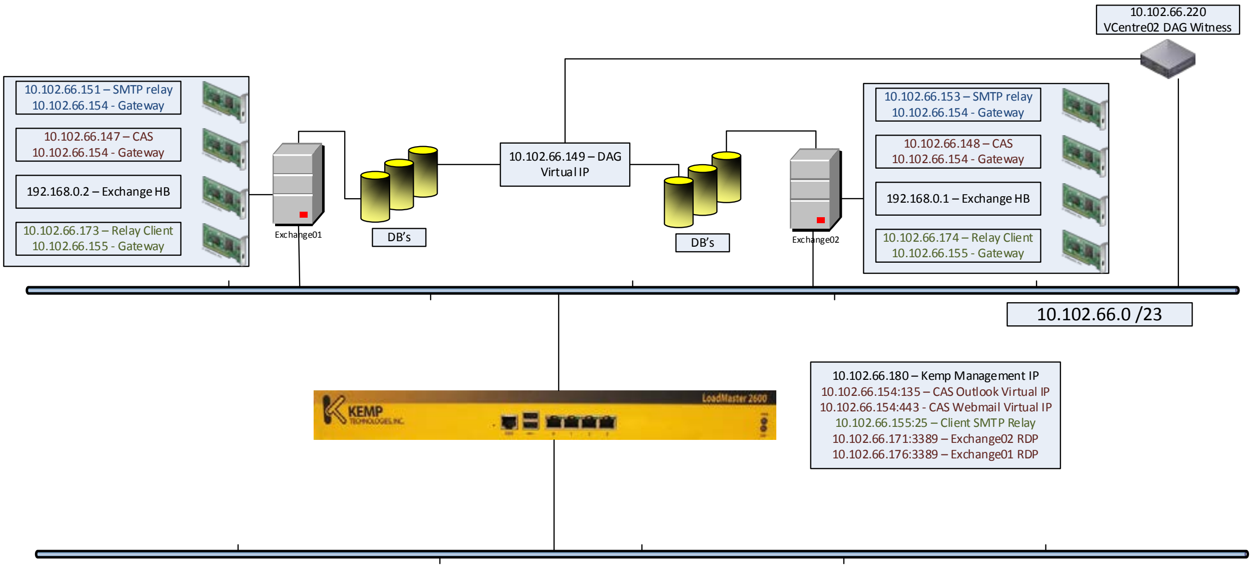
3.10 Electronic Mail

🚦	**Immediate**	**Achieve ISB1596 certification for current Exchange 2010 e-mail service. Commence the planning work required to enable the delivery of a Trust wide local MS Exchange 2013 e-mail service.**
	Tactical	**Upgrade Exchange 2010 to Exchange 2013, test and validate before ingesting HHCT users into the new solution.**
	Strategic	**Review the use of MS Exchange in conjunction with other designated software applications to maximise the benefits available from Exchange as part of the design of merged Trust service model.**

3.10.1.1 Current Position

PSHT

The e-mail solution at PSHT comprises an on premise Microsoft Exchange 2010 e-mail system that runs on virtualised servers deployed across DC1 and DC2 at PCH. This configuration ensures that the e-mail system is resilient and has no single point of failure, as shown in the diagram below. The e-mail traffic load is shared across both instances using a third party (Kemp) load balancer to optimise system performance and end user experience.


10.102.66.220
VCentre02 DAG Witness
10.102.66.151 – SMTP relay
10.102.66.154 - Gateway
10.102.66.147 – CAS
10.102.66.154 - Gateway
192.168.0.2 – Exchange HB
10.102.66.173 – Relay Client
10.102.66.155 - Gateway
Exchange01
DB's
10.102.66.149 – DAG
Virtual IP
DB's
Exchange02
10.102.66.153 – SMTP relay
10.102.66.154 - Gateway
10.102.66.148 – CAS
10.102.66.154 - Gateway
192.168.0.1 – Exchange HB
10.102.66.174 – Relay Client
10.102.66.155 - Gateway
10.102.66.0 /23
KEMP
LoadMaster 2600
10.102.66.180 – Kemp Management IP
10.102.66.154:135 – CAS Outlook Virtual IP
10.102.66.154:443 - CAS Webmail Virtual IP
10.102.66.155:25 – Client SMTP Relay
10.102.66.171:3389 – Exchange02 RDP
10.102.66.176:3389 – Exchange01 RDP

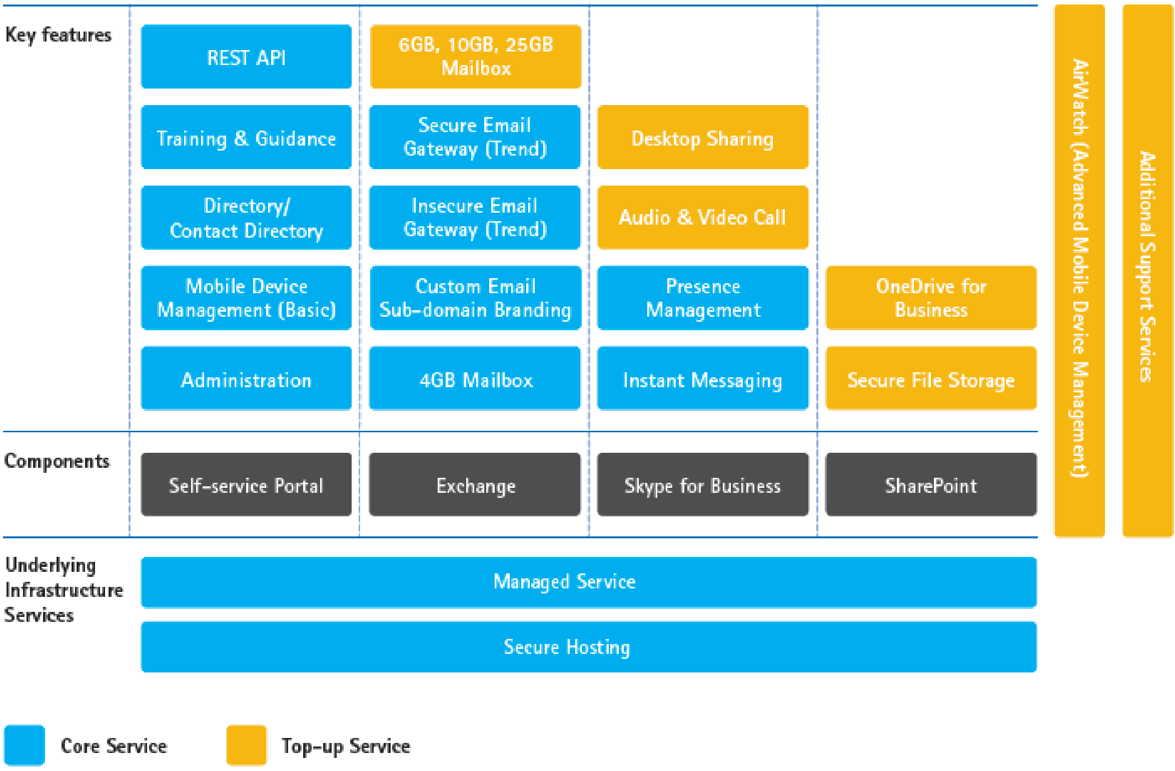
Users who require remote access to their e-mail solution can be provided with a mobile device running [redacted] MDM which uses the new [redacted] secure e-mail client that connects back via the [redacted] secure e-mail gateway. The alternative is to use the Microsoft Outlook Web Access client over a secure remote access link through a standard Internet browser.

The e-mail system at PSHT not only manages the vast majority of the Trust e-mail it also provides diary (calendar) management for all users including room and resource booking functionality. As part of the upgrade to Microsoft Exchange 2010 the Trust have ingested all of the old e-mail archive (.PST) files so that every user's e-mail archive is online. Additional work has been done to optimise e-mail storage by positioning e-mail onto the right tiers of the Storage Area Network (SAN) placing mailboxes, pagefiles and public folders on fast disk and other less used items such as leavers and archive, on slower disk.

Whilst Microsoft Exchange is the primary e-mail solution at PSHT it is not yet classified as a secure e-mail solution and so a modest number of Trust users also have an NHSmail account. All NHS Trusts are required to have secure e-mail that is compliant with ISB1596 in place by no later than June 2017. At this time work is underway for PSHT to achieve this certification with an expected certification date of November 2016.

HHCT

The e-mail solution at HHCT is the centrally provided NHSMail2 service provided by Accenture PLC under contract to the Health and Social Care Information Centre (now NHS Digital). NHSMail2 is a hosted service that operates from two commercial data centres in order to provide resilience and is accessed over the NHS N3 network. HHCT has around 2000 e-mail users, supports over 2500 mailboxes and maintains around 260 distribution lists. NHSMail2 offers a range of services as shown below, those services in the blue boxes form part of the centrally funded service whilst those in orange boxes are extras that users need to pay for directly.



3.10.2 Risks and Benefits

Reaching a conclusion on which e-mail solution to adopt for the merged Trust is a highly complex issue. Each solution offers a number of benefits and each comes with some risks and so the table below attempts to summarise these and show why the recommendation reached was chosen

On Premise Exchange Mail		NHS Digital NHSMail2	
Benefits	Risks	Benefits	Risks
Governance The on premise mail solution is managed by the Trust IT department and so FOI requests for mailbox content from both internal sources (e.g. HR/ TMB) and external source (Police/ FOI) can be initiated quickly as often in such cases time is of the essence.	**Funding** The cost of providing a Trust wide secure e-mail service is known to be around £20,000 per annum allowing for depreciation of hardware and on-going support of the application.	**Funding** At this time the basic NHSmail2 (as shown in the blue boxes above) is funded centrally. However, this was also the case of the Microsoft Enterprise License agreement that was funded centrally until 2012 at which time the full cost of Microsoft licensing was handed to the source organisations	**Governance** Access to the content of NHSMail2 mailboxes requires a request to be made to the NHSMail2 service desk after which the information can then be provided. At this time there is no published service level agreement on how long such requests will take to complete potentially causing significant delays.
Absence Experience shows that on many occasions access to a user mailbox, calendar or task is required at a time when the mailbox owner is absent. Trust IT can provide temporary access to such mailboxes and advise the mailbox owner when he/ she returns from the period of absence.	**Instant Messaging** As part of the Trust merger a new Microsoft EWA will be needed. At present, included in the PSNT EWA is Skype for Business which if carried forward into the new EWA would also provide Trust-wide Instant Messaging	**Instant Messaging** NHSMail2 includes the provision of Instant messaging as part of the core system. This allows on-line users to exchange text messages in real-time as if chatting on-line.	**Absence** Whilst NHSMail2 does allow mailbox users to authorise other registered users to have access to their mailbox there is no process at this time to override this for temporary access. Only the mailbox owner can change access rights.
Mailbox Sizes The on premise e-mail solution stores mailboxes on the Trust SAN and so mailbox size is only limited by the amount of storage available. Whilst managing mailbox growth is a function undertaken by IT there are users who genuinely need larger mailboxes.	**Mailbox Administration** In the merged Trust there will potentially over 5000 mailbox users and up to 8000 mailboxes in use. All these mailboxes need to be managed and all the associated changes administered in house. Whilst this work is a standard part of the current PSHT workload it is not performed at HHCT and so would need to be resourced.	**Mailbox Administration** Whilst in the merged Trust there will potentially over 5000 mailbox users and up to 8000 mailboxes in use, the primary role around mailbox administration will be fulfilled by the NHSMail2 service provider.	**Mailbox Sizes** NHSMail2 provide a maximum of 4Gb of mailbox storage within the core solution. Using the top up service NHSMail2 mailboxes can be increased in size however this is chargeable and the scale of charge has not yet been published. At this time there are around 135 e-mail users with a mailbox that is larger than the 4Gb allowance.
Patient Records In 2014 a coroners ruling was published advising that any e-mail concerning any clinical activity for one or more specific patients must be included in their patient record. Using the on premise e-mail solution and textual analysis it is possible for	**Service Risk** The provision of a high resilient e-mail service to over 5000 users with a high level of uptime requires investment in both IT staff and technology. The risk associated with the service therefore remains with the Trust.	**Service Risk** Whilst a third party hosted solution is not free from service risk, the investment made by NHS Digital around NHSMail2 is known to be significant. The advantage therefore to the Trust is that the service risk is transferred.	**Patient Records** At this time NHSmail2 does not offer any Application Programme Interfaces and so it is not possible to identify e-mail that relates to the patient record. In addition, there is no way to link NHSMail2 to the Trust EDM making it impossible to include NHSMail2 e-Mail in the patient record.

the Trust to identify such e-mail and forward for ingestion into the Trust EDM solution for inclusion in the patient record.			
Local Integration One of the key tasks facing the new Trust is the need to redesign services and to engender far greater collaborative working. As there are many functions with Microsoft Exchange that can be used to support this agenda there is discernible benefit to be gained from integration with local systems.	**Secure E-mail (NHS)** The Trust is required by NHS Digital to adopt a secure e-mail system that is compliant with ISB1596 by no later than June 2017. Whilst PSHT is well on the way to achieving this, the required standard has not yet been reached. At part of a merged Trust, it will also be necessary to have the new mail system certified as compliant with the secure e-mail standard.	**Secure E-mail (NHS)** NHSMail2 provides level 2 secure e-mail that is fully compliant with ISB1596 as a core part of their service offering.	**Local Integration** Unfortunately, NHSMail2 only offers integration into existing Microsoft products such as SharePoint and Skype for Business. There is no means to integrate NHSMail2 into any Trust clinical or business systems.
Collaborative Working As noted above far greater collaborative working is a key requirement outlined in the merger OBC. At this time there are a number of sophisticated collaboration tools such as Cisco Jabber that enable this in a health context. Benefits from a product such as Jabber include: Far greater control over telephone call routing in particular for clinical staff; can be deployed Trust wide on one or more mobile devices providing anytime and place real time communications; can enhance the electronic patient record in events such as MDT; can be used for remote patient video conference up to and including remote OP appointments. Currently this is only available on a local copy of Microsoft Exchange.	**Secure E-mail (Non NHS)** It is clear that secure e-mail to non NHS recipients such as patients will be required in the merged Trust. Local Microsoft Exchange can be integrated with 3rd party software that provide this functionality at a cost.	**Secure E-mail (Non NHS)** NHSMail2 provides tools to enable the transmission of secure e-mail to non NHS recipients such as patients as a core part of their service offering.	**Collaborative Working** At this time NHSMail2 only offers integration into two Collaboration tools these being SharePoint and Skype for Business. Whilst these both have some value there are a number of other third party tools that offer far greater functionality in a complex environment such as healthcare.
E-Mail Archiving PSHT has already invested in technology to provide a local e-mail archive and as part of the merged Trust this would be expanded. This approach to arching means that Trust staff can recall e-mail from the previous moth or year both quickly and easily without the need for IT staff		**Presence** One useful feature of the new NHSMail2 is its national directory and the ability to display those users who are signed into the system. Knowing that a colleague in another health or social care organisation is on-line facilities quick communication using either Instant Messaging or	**E-Mail Archiving** A review of NHSMail2 has failed to find any reference to long term e-mail archive. It is clear that users can keep e-mail on-line for as long as they wish subject to the size of their mailbox. Any mailbox over 4Gb in size is subject to a charge and deleted e-mail is only retained for 180 days as

intervention. For all but the most basic of e-mail users accessing archived e-mail is a fairly routine task.		Video Conferencing.	standard. On this basis we feel that NHSMail2 has not provided a long terms solution for the archiving of older e-mails.

In creating this risk/ benefits table and in reaching a decision of the optimum option for the merged Trust to adopt, input has been received from additional consultants outside the immediate PSHT and HHCT engagement. These include:

Michael Bone, former Director of ICT at Great Ormond Street Hospital
Jon Reed, former Director of IM&T at the Royal Marsden NHS Trust
Ian Hall, former Chief Technology Officer at BMI Hospitals
Matthew Douglas, former NHS IT Operations Manager and now IT Director at Rayner
Clive Booth, former IT Operations Manager at Royal Sun Alliance Insurance and a Microsoft MCSE

Whilst every effort has been made to be comprehensive around the identification of risks and benefits, it is acknowledged that a risk and/ or benefit that is unknown to the Methods team or did not arise during the discovery phase, may exist and so may not be included in the table.

3.10.2.1 Options

The options to address this issue are as follows:

1	**Do Nothing**
At this time the two Trusts have to very different e-mail solutions deployed. As e-mail is a key collaboration suite moving forward the Trust must move to a single integrated solution in order to maintain operational capability. In addition, as part of any post-merger service re-design the successful use of collaboration tools will be central to the supporting services that will underpin the revised clinical service model. **On this basis the Do Nothing option is rejected**	
2	**Adopt NHSMail2 Trust Wide**
The Trust could choose to adopt NHSMail2 Trust wide and this would provide a fully operational e-mail based collaboration service. However, there is a number of key issues, in particular around the integration of NHSMail2 with unified communications, mobile device security and most notable clinical systems (such as EDM) that are more difficult or simple not achievable at this time. Whilst the central funding of NHSMail2 is a strong driver, the need for the Trust to significantly redesign operational and clinical services to drive up efficiencies, optimise back office and reduce unit costs are less easy to achieve with NHSMail2. **On this basis this option is not recommended.**	
3	**Secure on premise MS Exchange Trust Wide**
The Trust could choose to extend secure on premise MS Exchange Trust wide as this would provide a fully operational e-mail based collaboration service. However, moving forward, the Trust need to significantly redesign operational and clinical services to drive up efficiencies, optimise back office and reduce unit costs. The ability to integrate MS Exchange with unified communications, mobile device security and most notable clinical systems (such as EDM) are key enablers to achieving this aim. In addition, the improved agility and governance provided by an on premise solution further enhance this option. **This option is recommended as both a tactical and strategic solution.**	

3.10.2.2 Costs

The costs of addressing the e-mail issues is as follows:

Title	Capital	Revenue
Do Nothing	£0.00	£0.00
Adopt NHSMail2	£53,000.00	£33,000.00
Secure on premise MS Exchange Trust Wide (See Note 1)	£13,750.25	See Note 2

A detailed statement of work for the extension of MS Exchange is provided in a separate document held by the Head of IT.

Note 1: The cost data provided against option 3 is based upon an upgrade of the existing PSHT Exchange 2010 solution to a Trust wide Exchange 2013 solution. Upon review it was agreed that system resilience, e-mail archive management and some functionality already provided by NHSMail2 would be far better served by moving to Exchange 2013 as part of the Trust merger.

Note 2: There will be a revenue cost for these licenses however, as these will form part of the merged Trust Microsoft Enterprise Wide Agreement (EWA), we are unable to provide a meaningful figure as part of this review.

3.10.2.3 Recommendations

Immediate: Achieve ISB1596 certification for current Exchange 2010 e-mail service. Commence the planning work required to enable the delivery of a Trust wide local MS Exchange 2013 e-mail service.

Tactical: Upgrade Exchange 2010 to Exchange 2013, test and validate before ingesting HHCT users into the new solution.

Strategic: Review the use of MS Exchange in conjunction with other designated software applications to maximise the benefits available from Exchange as part of the design of the merged Trust service model.

3.11 Integration Services

🚦	Immediate	There are no immediate infrastructure requirements for Integration Services
	Tactical	In line with the Clinical System consolidation plan, review all existing system interfaces at HHCT and commence planning for migration to Ensemble. (Note dependencies)
	Strategic	Assess options for expanding the use of the Ensemble Integration Engine. Review possible addition of InterSystems Healthshare as a portal in-line with NHS Digital 2020.

3.11.1.1 Current Position

PSHT

The integration engine at PSHT is an enterprise grade solution called Ensemble from InterSystems Corporation and is one of the leading integration engines in use today. The Ensemble engine sits on the PSHT Microsoft SQL Server cluster and supports some 18 electronic interfaces linking business and clinical systems together so that data flows where it is needed when it is needed. The use of a SQL Cluster platform for the Ensemble database combined with a virtual server for the application provides a high level of resilience, keeping the integration engine running at all times. There are four members of the Information Management team who are proficient with Ensemble and PSHT have utilised its extensive functionality to support healthcare delivery across the Trust.

The most obvious example of this is the PSHT in-house e-Track application that is a clinical workstation application providing near real-time data to clinical teams in primary care areas such as A&E, Hospital Wards and Outpatients along with a myriad of other clinical spaces. It is well liked by clinical staff and PSHT have plans to continue it development going forward.

In our opinion Ensemble is a world class integration engine deployed by PSHT in an exemplary manner and exploited to the best of its abilities and so very suitable for continued use in the merger Trust.

HHCT

The integration engine at HHCT is also an enterprise grade solution called Rhapsody from Orion Healthcare. It too is one of the leading integration engines in use today and there are many examples across the NHS in daily use. Rhapsody like Ensemble, uses Microsoft SQL server for its message database with the application running on a virtual server. HHCT have one member of staff who is proficient with Rhapsody and to date, have developed some six electronic interfaces linking key clinical systems together and supporting the timely provision of clinical data to operational teams.

> Risks
> The reliance on a single member of staff with the proficiency to manage a key technological component is a modest risk to the Trust. This risk is mitigated in part through support and maintenance contract but provision of a second skilled resource would significantly reduce this risk.

In our opinion Orion Rhapsody is also a world class integration engine which, from an infrastructure perspective, has been well deployed and so suitable for continued use in the merged Trust.

3.11.1.2 Options

Each Trust is in a strong position, each having a world class integration engine, each of which would be more than capable of providing Trust wide systems interfacing in the merged Trust. However, the larger team of staff proficient in its use and the level to which Ensemble has been developed at PSHT makes a stronger case to retain Ensemble in the medium to long term. By taking this approach, there is also an opportunity to strengthen the emerging team further, by adding the SQL Server Database and Integration engine skills of the member of staff at HHCT into an enlarged and combined team as part of the merger. Whilst some cross training will be required, the principles of systems interface development are consistent across both integration engines. In addition, the HHCT member of staff also has considerable SQL Server Database skills that would be a welcome addition to the nascent team.

3.11.1.3 Costs

There are no infrastructure costs to deploy Ensemble across the merged Trust. Work will be required to redevelop the existing Orion Rhapsody interfaces currently in use at HHCT. However, the nature of this work and any costs should be reported in the clinical systems review also being undertaken at this time.

The annual Orion Rhapsody support and maintenance contract runs from 20th October each year for 12 months with an annual revenue value of £18,810.00. It should be possible to cease this from October 2018 with the resulting revenue saving.

3.11.1.4 Recommendations

Immediate: There are no immediate infrastructure requirements for Integration Services

Tactical: Once new external links are in place and in-line with the Clinical System consolidation plan, review all existing system interfaces at HHCT and commence planning for migration to Ensemble.

Strategic: Assess options for expanding the use of the Ensemble Integration Engine. Review possible addition of InterSystems Healthshare as a portal in-line with NHS Digital 2020.

Note: Lincoln CCG have adopted Healthshare as a health community portal within there STP. This therefore presents an opportunity for the merged Trust who receive approximately 40% of the business at Peterborough and Stamford Hospital from Lincolnshire to improve the electronic exchange of clinical information across this health community and with this important CCG.

3.12 Resilience

🚦	Immediate	Procure and commission technology component upgrades to deliver improved infrastructure resilience.
	Tactical	Once the new structure of IT has been confirmed develop updated Business Continuity plans. Focus on how IT services would be delivered in the face of business interruption.
	Strategic	When the new service model for the merged Trust is known undertake a full Business Impact Analysis and developed updated Disaster Recovery plans, in particular for priority one systems or services.

3.12.1.1 Current Position

PSHT

The team at PSHT have taken a practical approach to resilience with the result that, where ever possible, appropriate technology has been deployed to minimise the risk of failure arising from the loss of a single instance of technology. Examples include devices with multiple power supplies, network interfaces, controllers and key components; the provision of UPS, air handling, fire detection and environmental monitoring in network hub rooms; and N+1 approach to all key data centre components; a network built around two cores each of which is linked to every hub room and the wide spread use of data replication across its storage area networks.

Therefore, with the exception of Trust servers only being connected to one core switch (see section 3.3.1 for further details) it is our opinion that PSHT has a satisfactory level of resilience across its IT service.

HHCT

The team at HHCT have implemented resilience in high risk areas where the IT funding envelope has allowed. The challenge around resilience at HHCT comes in two parts: the first where resilient components do exist but are no longer fit for purpose (for example hub room UPS); the second, where resilience is needed but has not been provided (for example SAN data replication). Clearly there are some areas of good practice, for a network built around two cores each of which is linked to every hub room but this is not consistent across the IT service.

This infrastructure review contains a number of recommendations around investment in technology upgrades which will, if implemented, address these concerns. However, at this time it is our opinion that HHCT lacks the necessary level of resilience required in a complex environment such as a hospital and so the IT service is running at risk.

3.12.2 Business Continuity

3.12.2.1 Current Position

PSHT

PSHT has a well-defined and detailed BCP plan that includes some of the political, social and human issues that have impact on the continued delivery of IT services. Key locations are clearly identified and a sound command structure has been included. However, the aim of a Business Continuity plan is to outline how the IT Department would continue to provide the services that operate from its key locations should these no longer be operable.

For example: if the IM&T Ground Floor workshop is no longer operable what services are provided out of the workshop? How business critical is each service? Can some or all of these services be provided from an alternative location? In particular, those that are most business critical. If they can be provided where and how?

Whilst the plan has many good features, it needs to focus more on how IT services would continue as a business function with one or more service locations inoperable. However, care needs to be taken as clearly a large business interruption may see IT focus more heavily on the recovery of technology services than the continued provision of the normal IT service.

HHCT

No specific Business Continuity documentation was assessed by the Methods team as part of this Infrastructure review.

3.12.3 Disaster Recovery

3.12.3.1 Current Position

PSHT

PSHT has a well-defined and detailed "Serious IM&T Incident Procedure" that sits alongside the IT Recovery Plan. The former clearly defines what constitutes an incident and this is coupled to a flow chart that shows the steps and escalation points. The document shows the incident command structure including the definition of roles and responsibilities. However, the team comprises all the senior managers within IT with the risk that should the recovery take more than 12 hours there is no second team to come in and continue the recovery at the point where the starting team are due to be relieved. The plan continues with reference to recovery red boxes aligned to the BCI standard containing information and material that are germane to the recovery. There are also good sections on Management Considerations and Communication which cover much of what is needed.

What is missing is information on staff call out, an index of supplier information, any reference to backup media in terms of location, access and secondary technology and any detail on how the recovery itself would be achieved.

HHCT

HHCT has an up to date IT Disaster Recovery plan with a good opening section on risk that includes a master list of systems and suppliers. However, this is provided as an electronic link to an XL sheet rather than as a hard copy (e.g. Appendix) with the risk that should the SharePoint system be down there would be no access to the data. Objectives and Responsibilities are also included but only at very high level.

3.12.4 Summary

RESILIENCE

All of the resilience issues are covered in detail in the body of this Infrastructure Review including recommended options and the associated costs. If the proposed investment in technology is undertaken, the merged Trust will be very well placed to deliver high class, technology enabled healthcare services, underpinned by high performance and resilient IT infrastructure.

BUSINESS CONTINUITY

Once the new service delivery model for the merged Trust is known it would be a good time to revisit the IT Business Continuity plan. Aligned to the new service model and cognisant of the new structure of IT services Trust wide, a new BC plan can be made, building on the good work already done for the PSHT plan. The new BC plan should be built around the BCI PAS56 model and be focussed on the continued delivery of IM&T services in the event of business disruption.

DISASTER RECOVERY

This IT infrastructure review includes a number of proposals that will significantly change the topology of IT in the merged Trust. Alongside this, Libretti Health have been reviewing the future of clinical applications with recommendations as to what should be deployed across the merged Trust. Once these are known the Trust would greatly benefit from a formal Business Impact Analysis, as this will not only aid the formation of Business Continuity plans across the Trust but will also drive the order in which key IT systems are recovered. As part of this development, the Trust may wish to consider creating specific system and/ or service recovery plans for all of its priority one systems.

3.12.4.1 Options

As both BC and DR plans are mandated for NHS organisations as part of the annual compliance audit, there is no option but to create new plans once the shape of the merged Trust is known. However, given the significant role played by IT in the delivery of healthcare services, we would recommend that the Trust engage a BCI qualified professional to ensure the coverage and content of the new plans comply with published standards.

3.12.4.2 Costs

The cost of Professional Services to support the development of Business Continuity and Disaster recovery plans are included in section 3.15 on Professional Services.

3.12.4.3 Recommendations

Immediate: Procure and commission technology component upgrades to deliver improved infrastructure resilience.

Tactical: Once the new structure of IT has been confirmed develop updated Business Continuity plans. Focus on how IT services would be delivered in the face of business interruption.

Strategic: When the new service model for the merged Trust is known undertake a full Business Impact Analysis and developed updated Disaster Recovery plans, in particular for priority one systems or services.

3.13 Security and Governance

🚦	Immediate	**Recruit Information Security Support Officer**
	Tactical	**Build new Information Security model aligned to ISO: 27001 for merged Trust. Update policies, controls, procedures and reporting against the new model. Mandate annual staff Security and Governance training.**
	Strategic	**Review security threats as data flow across the Trust electronic borders increases in line with NHS Digital 2020.**

3.13.1 Structure

PSHT

The security structure at PSHT is largely modelled on the International Security standard ISO: 27001. The Trust has an Information Security Forum that formulates Information Security Policy and Controls which in turn reports through an Integrated Governance Committee to the senior team. Alongside the Information Security Forum, the Trust also has a Health Records and Governance Committee which manages all of its Information Governance issues with good representation from both Information Management and Technology. The delivery of Information Security on the ground is overseen by a dedicated Information Security Officer who reports directly to the Head of Information Technology.

HHCT

Information Security at HHCT largely falls to the IT Operations Manager with support from the Network and Data Centre Managers. Information Governance is managed within Health Records who have allocated resource; both are overseen by the Information Governance Committee. The IT Operations Manager and the EPR Programme Manager have seats on the IG Committee covering technical security and security for Clinical Systems.

3.13.2 Standards

Both Trusts follow the Information standards set out in the NHS Information Governance toolkit and each has reached level 2 in terms of its compliance. Formal change control exists at each Trust and both Trusts operate varying levels of information security audits. Security Incident Management procedures are in place at both Trusts and are integrated with the IT Service Desk.

3.13.3 Policy

PSHT

There is a formal Information Security Policy at PSHT that is well structured, it is compromised of strategic security policy statements in the body of the document, supported by more policy instruction and compliance measures in a series of appendices. The appendices also breakout into a series of detailed user Code of Practice documents that provide practical guidance on a wide range of Information Security Issues. All of these documents have an assigned author and a policy expiry date which is policed by the Information Security manager and the Trust's Compliance Manager.

HHCT

HHCT also has an Information Security policy that sets out objectives, responsibilities, legal compliance and lists some 12 related policies that cover a mixture of Information Governance and Information Security topics. However, the document lacks any strategic security policy statements and was last reviewed almost two years ago. Seven of the related policies were reviewed and all provide basic guidance in the topic area, with several being detailed and comprehensive and some being more general. The overall size of the HHCT team and the lack of a dedicated Security Officer are reflected in what the team has been able to achieve in terms of policy documentation.

3.13.4 Procedure

PSHT

There is a comprehensive range of Information Technology procedures at PSHT many of which include reference to Information Security where this is appropriate. All of those that were reviewed were found to be well structured and detailed with suitable cross reference where required. Those procedure documents that were reviewed have an assigned author and a policy expiry date which is policed by the appropriate Senior Manager within IT and subject to review by the Head of IT.

HHCT

HHCT has a number of Information Technology procedures that are documented. Where procedure documents have been generated they are generally fit for purpose but again the overall size of the HHCT team is reflected in what the team has been able to generate in terms of Information Security within IT procedure documentation.

3.13.5 Reporting

PSHT

There is a well-defined Information Security reporting process that incorporates the Trust Security Incident Management procedure. All risks are reported via the IT Security Officer and any reported security risk with a value of 12 or above (as defined with the Trust Risk Management policy) is immediately alerted to the Head of IT. Any high risk items with a risk score of 20 or more is immediately escalated to the Trust Management Board via the Director of Finance. Routine security reporting is reviewed by the Information Security Forum and a summary report is also routinely presented to the Integrated Governance committee.

HHCT

At HHCT routine security reporting is reviewed by the Network Manager and IT Operations Manager with a summary report being presented to the Information Governance committee for review by the Senior Information Risk Officer (SIRO). Security Incident reporting is also reviewed initially by the Network Manager with first stage escalation to the IT Operations Manager and second stage to the Trust Board via the Director of Finance.

3.13.6 Summary

The security model used at PSHT is closely aligned to ISO: 27001 and one of the best we have seen across the NHS. There are examples of best practice across each area of Information Security management and it is clearly seen as being a key function for the safe delivery of healthcare services. Whilst the security at HHCT is satisfactory, the lack of a dedicated security officer and the modest size of the IT team has limited what can be achieved. There are also examples of good practice within the security domain at HHCT.

The demands of NHS Digital 2020 will see an ever increasing use of electronic information both across and outside the electronic borders of the Trust. As the NHS introduces patient portals holding ever more complex clinical data, and as the exchange of such data across Health and Social care centres is driven forward, the need for advanced security will only continue to grow,

Changes in such electronic borders increase the risk of attack and these days, reports of cybercrime are almost a daily occurrence. Indeed, there are frequent reports of phishing, social engineering and ransomware attacks occurring right across the public sector. As a result, a clear information security governance structure, strong information security policy, advanced security controls, regular testing and mandatory staff training (at least annual) are key to a secure future.

3.13.6.1 Options

In the merged Trust we would strongly recommend the provision of a Security Support Officer to work under the existing Security Officer as part of the merged Trust. We believe that a Trust of the size to emerge from the merger will be unable to sustain the required level of Information Security with just the existing resource. We have therefore included this in section 3.14 on Staff Resources and Structure.

3.13.6.2 Recommendations

Immediate: Recruit Information Security Support Officer.

Tactical: Build new Information Security model aligned to ISO: 27001 for merged Trust.
Update policies, controls, procedures and reporting against the new model.
Mandate annual staff Security and Governance training.

Strategic: Review security threats as data flow across the Trust electronic borders increases in line with NHS Digital 2020.

3.14 Staff Resources

3.14.1.1 Current Position

PSHT

The Information Technology team at PSHT (as shown in the diagram below) is based upon a sound structure and has sufficient staff to safely deliver Information Technology services across the Trust. The number of staff is sufficient to provide cover for all forms of absence and has enough depth to ensure that there is no complete reliance on individual members of staff.

DIAGRAM REMOVED

The organisational structure of the team provides a strong senior management layer with the only observation being that the structure does not include a designated Deputy Head of IT role. Whilst this may not be perceived as a risk currently, we feel that it may require a further review as the shape of the merged Trust takes place.

Under the senior management layer services are provided by teams of staff aligned to the Information Technology Infrastructure Library, which is a recognised set of best practice guidance for IT service management (ITSM) that focuses on aligning IT services with the needs of business.

HHCT

The Information Technology team at HHCT (as shown in the diagram below) is the minimum structure that is required to deliver Information Technology services across the Trust. The number of staff is small and in our view struggles to provide cover for all forms of absence. In the three key areas of Database & Integration, Network and Data Centre there is heavy reliance on individual members of staff to sustain the service.

DIAGRAM REMOVED

3.14.1.2 Future Structure

A proposed structure for the newly merged Trust fully integrated IT department is shown below.

DIAGRAM REMOVED

The design of the new structure provides strong leadership with a senior manager heading each of the cores teams. These in turn are then broken down into smaller operational teams and where these teams warrant it, there is a Team Leader role included. On this basis we feel that the proposed structure provides sufficient personnel in the teams to deliver a safe and functional IT service with one exception.

In the structure above there is only one member of staff assigned to the role of ICT Security. The process of merging two NHS Trust organisations together generates a very substantial amount of change, in particular for ICT disruption of the security perimeter. On top of this, each organisation has attained different standards and operating procedures in respect of security and these need to be harmonised. In addition, the new organisation will include two acute hospitals and so it is our opinion that ICT security should comprise two roles. An ICT Security Manager at Band [redacted] (as shown above) and an ICT Security Officer at Band [redacted] to support the manager and deliver the security agenda across multiple sites.

[redacted]

3.15 Professional Services

As noted throughout the document the process of merging two NHS Acute Trusts into one fully operational organisation is a very substantial and complex process that spawns significant work under the change agenda. However, during this change period, the nascent organisation needs to continue with its primary mission – to deliver high quality and safe healthcare services to its patients. It is therefore necessary to engage additional resource to enable the change whilst minimising the impact on the operational service. The table below includes all of the professional services that we believe will be required to achieve this:

Area	Resource	Time	Cost
Data Centre	Consultant to build commercial hosting output based specification	30 days @ £750 per day	£22,500
Wired Network	[redacted] Engineer to install and commission aggregation switches at PSHT and HHCT	10 days @ £850 per day	£8,500
Remote Access	Migrate HHCT users to [redacted] & introduce PSHT Remote Access model (see note 1)	NHS Band 6 for 1 Year	£30,357
Management Platform	[redacted] Consultant to configure system across merged Trust	3 days @ £1,150 per day	£3,450
Unified Communications	Network Engineer support for Unified Communications Project	Shared Resource with Remote Access above	
Voice Services	Cabling Company to install 20 pair copper cables from frame to 23 hub rooms	£1200 per hub room	£27,600
	PABX Engineer to install analogue PABX and operator consoles plus link to network	5 days @ £750 per day	£3,750
	[redacted]	30 days @ £1000 per day	£30,000
	[redacted]	15 days @ £850 per day	£12,750
[redacted]	[redacted]		
	Professional Services to build and configure IVR for merged Trust	Fixed Price Package	£15,000
Network Addressing	Network Engineering Support for changes to Trust Network Addressing	Shared Resource with Remote Access above	
Desktop	Contract Resource to handle rollout of 700 new personal computers at HHCT	NHS Band [redacted] for 2 Years	£42,104
	Contract Resource to migrate 1400 users onto [redacted] PC Protection Suite	Shared Resource with Desk PC rollout above	
Compute	Systems Engineer to install 4 Node ESXi VM platform at PSNT	3 days @ £850 per day	£2,550
	Systems Engineer to install 4 Node ESXi VM platform at HHCT	3 days @ £850 per day	£2,550
	Contract Resource to implement consistent server management processes Trust wide	NHS Band [redacted] for 2 Years	£48,608
Storage	Storage Area Network Engineer to upgrade [redacted] SAN at PSHT	3 days @ £850 per day	£2,550
	Storage Area Network Engineer to upgrade [redacted] SAN at HHCT	3 days @ £850 per day	£2,550
	Storage Area Network Engineer to install new [redacted] SAN at HHCT	7 days @ £850 per day	£5,950

Service Desk	Contract Resource to migrate service desk into out of [redacted]	NHS Band [redacted] for 6 months	£9,076
Active Directory	Microsoft Engineering Support for AD migrate in particular new schema design and user migration tools	20 days @ £1000 per day	£20,000
E-Mail	Microsoft Engineering Support for e-mail Upgrade and expansion to HHCT	20 days @ £1000 per day	£20,000
Resilience	Consultancy Services to build IM&T Business Continuity Plan	20 days @ £750 per day	£15,000
	Consultancy Services to deliver a post-merger Trust wide Business Impact Analysis	32 Days @ £750 per day	£24,000
	Consultancy Services to build IM&T Disaster Recovery Framework and one example plan	20 days @ £750 per day	£15,000
Security and Governance	Contract resource to consolidate Trust Information Security Policies and Procedures	NHS Band [redacted] for 1 year	£35,225
			£494,720
	VAT/On costs for NHS Staff @ 20%		£98,944
	TOTAL COST OF PROFESSIONAL SERVICES		**£593,664**

4. Infrastructure Cost Summary

The table below brings together all of the costs in terms of technology investment and professional services to generate an Infrastructure Cost Summary. The table is presented in the same order as the body of the Infrastructure Review with a total cost for the Trust merger from an Infrastructure cost perspective at the base. Where there are options resulting in a range of costs the recommended option is the one included in the cost summary. The table presents the cost information in two columns labelled Capital and Revenue. Capital is defined as any cost that is a one off cost and in NHS accounting terms include onetime revenue. Revenue is defined as a cost that is recurrent, usually on an annual basis without a declared termination date. Where this is not the case and a termination date is known this will be noted as a footnote to the table.

Index	Title	Capital	Revenue
3.2.1	Data Centre – Commercial Hosting Centre	£26,785.00	£302,504.23
	Professional Services	£22,500.00	£0.00
3.2.2	Hub Rooms – HHCT UPS Refresh	£92,000.00	£23,600.00
3.3.1	Wired Network Core – Aggregation Switches	£110,700.50	£10,288.15
	Professional Services	£8,500	£0.00
	Wired Network Edge – Edge Switch Refresh	£292,188.82	£0.00
3.3.2	Wireless Network	£20,000.00[1]	£0.00[1]
3.3.3	Network Perimeter	£25,000.00[2]	£0.00[2]
3.3.4	External Links – 10Gb link PCH to HH (5 Years)	£42,100.00	£30,000.00
	External Links – 1Gb link SRH to HH (5 Years)	£16,800.00	£30,000.00
3.3.5	Remote Access – [redacted] Package	£19.925.00	-£15,197.60
3.3.6	Management Platform – [redacted]	£12,470.00	£1,248.00
	Professional Services – System Configuration	£3,450.00	£0.00
3.4.1	VoIP – 2nd [redacted]	£7,890.00	£1,100.00
	Consultancy to plan merger [redacted]	£30,000.00	£0.00
	[redacted]	£12,750.00	£0.00
	VoIP – Install Analogue PABX	£12,000	£2,400
	Cabling Services to install 20 pair copper cables	£27,600.00	£0.00
3.4.3	Paging	£101,220	£10,000
3.4.4	Switchboard – Extend IVR Trust Wide	£66,440.00	£0.00
	Professional Services for IVR	£15,000.00	£0.00
3.6.1	Desktop/Laptop – Capital Sum and budget uplift	£320,000.00	£300,000.00[3]
	Contract Resource to rollout 700 new PC's	£42,104.00	£0.00
3.6.3	Security Suite – [redacted]	£30,000	
3.7	Compute – ESXi compute platform for PSHT	£55,236.21	£5,590.17
	System Engineer to install 4 Node ESXi	£2,550.00	£0.00
	Compute – ESXi compute platform for HHCT	£55,236.21	£5,590.17
	System Engineer to install 4 Node ESXi	£2,550.00	£0.00
	Storage – SAN Upgrade for PSHT	£56,187.57	£6,019.27
	Storage Engineer to upgrade [redacted] SAN	£2,550.00	£0.00
	Storage – SAN Upgrade for HHCT	£324,432.38	£29,197.23
	Storage Engineer to upgrade [redacted] SAN	£2,550.00	£0.00
	Storage Engineer to install new [redacted] SAN	£5,950.00	£0.00

	Database – SQL Server Upgrade	£0.00	£162,000.00
3.8	Service Desk – Extend [redacted] to HHCT	£56,500.00	£15,535.72
	Contract Resource to migrate onto [redacted]	£9,076.00	£0.00
3.9	Active Directory		
	Microsoft Engineer to support new AD	£20,000.00	£0.00
3.10	Electronic Mail		
	Microsoft Engineer to support E-Mail Migration	£20,000.00	
3.11	Integration Services – [redacted]	£2,000	
3.12	Resilience - Consultancy Services - IM&T BC Plan	£15,000.00	£0.00
	Consultancy Services – Full BIA	£24,000.00	£0.00
	Consultancy Services – IM&T DR Framework	£15,000.00	£0.00
3.13	Security & Governance		
	Contract Resource – to build new Security Policies & Procedures	£35,225.00	£0.00
	Total Infrastructure Net Costs for merged Trust	£2,041,541.69	£919,875.35
	VAT/Staff on Costs @ 20%	£408,308.34	£183,975.07
	TOTAL INFRASTRUCTURE COSTS FOR MERGED TRUST	**£2,449,850.03**	**£1,103,850.42**

1. We have included a provisional sum of £20,000 as a wireless network survey is required before any wireless network upgrade can take place.
2. A site survey by WAN providers is required before a meaningful price can be reached and so a provisional sum of £25,000 has been included
3. Contract Resource for PC rollout is based upon IM&T receiving both the capital and revenue sums proposed.

Appendix A

Data Centre Tier Standards

The data centre review for all locations has been undertaken against the Telecommunications Industry Association standard number 924 entitled "Telecommunications Infrastructure Standard for Data Centres" issued originally in May 1998 and updated recently to version 2 as issued in March 2010. This widely recognised standard provides data centre models in four tiers which in summary are as follows:

Tier One: Basic Site Infrastructure

A tier one data centre has non-redundant capacity components and a single, non-redundant distribution path serving communications and computing equipment. Tier one sites are susceptible to disruption from both planned and unplanned activities including human error that will cause a loss of service. The unplanned outage or failure of any single component will impact communications and/ or computing equipment. The whole site infrastructure has to be shutdown to perform safety checks, undertake maintenance or install new components.

Tier Two: Redundant Site Infrastructure

A tier two data centre has redundant capacity components combined with a single, non-redundant distribution path serving communications and computing equipment. Tier two sites are able to have redundant capacity components removed from service without causing a service disruption. However, they remain susceptible to disruption from both planned and unplanned activities that will cause a loss of service. An unplanned outage or failure of any single component may impact communications and/ or computing equipment and like tier one sites the whole site infrastructure has to be shutdown to perform safety checks, undertake maintenance or install new components.

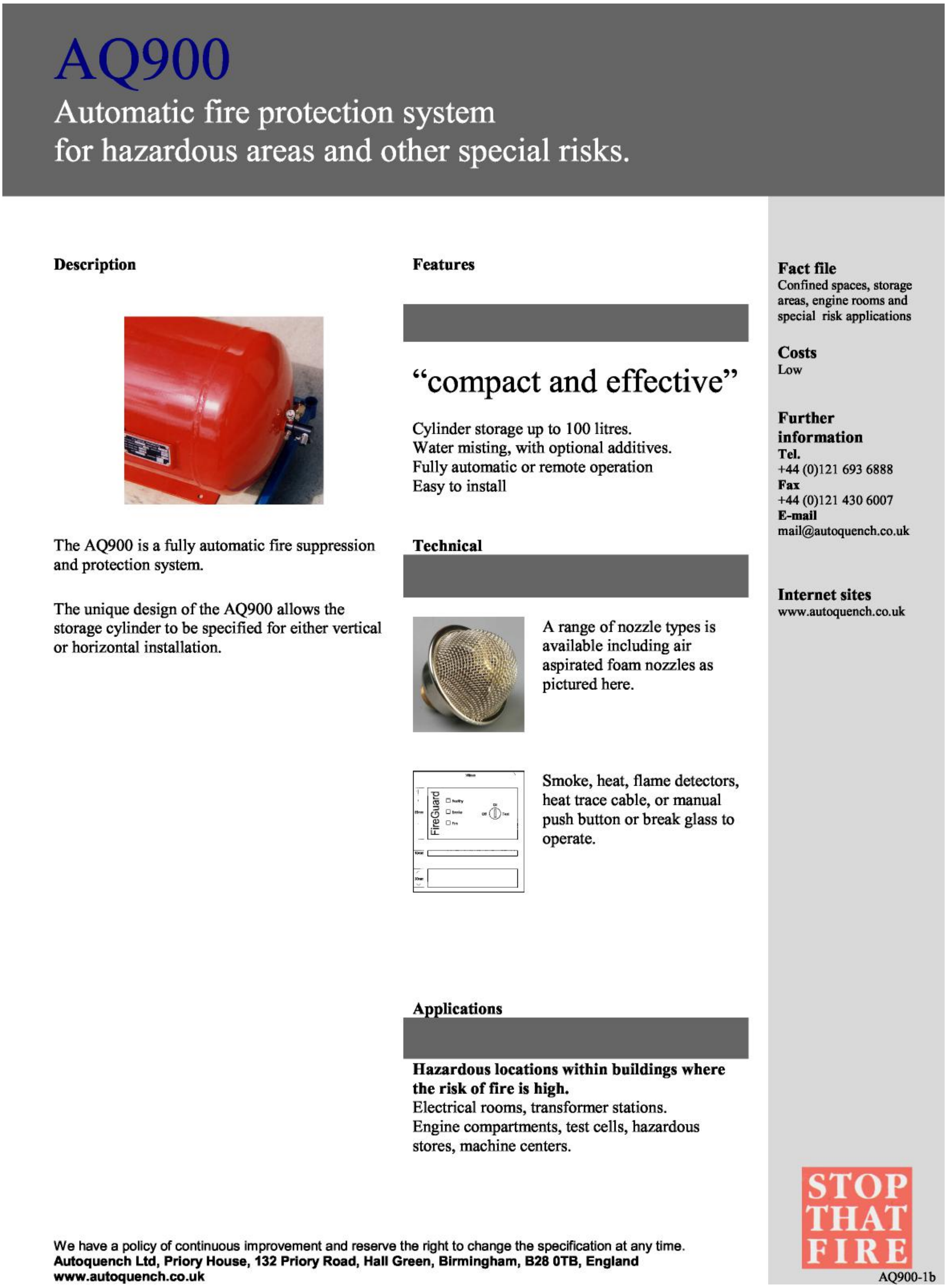
Tier Three: Concurrently Maintainable Site Infrastructure

A tier three data centre has redundant capacity components and multiple independent distribution paths serving communications and computing equipment. All equipment has dual power feeds and power supply units that can be switched seamlessly without affecting the service provision. Any capacity component and/or element in the distribution path may be removed from service on a planned basis without impacting any communications and computing equipment. Tier three sites are however susceptible to disruption from unplanned activities including human and operational error. As a result, unplanned outage or failure of either capacity components or elements of the distribution path will impact the service provision. However, planned site infrastructure safety checks, maintenance or installation of new components can be undertaken safely using the redundant components to support communications and computing equipment.

Tier Four: Faults Tolerance Site Infrastructure

A tier four data centre has multiple, independent, physically isolated systems that provide redundant capacity components and multiple, independent, diverse and active distribution paths serving all communications and computing equipment. In a tier four data centre, a single failure of any capacity component or any element of the distribution path will not impact the communications and computing equipment. In addition, the equipment that provides capacity and distribution is configured to automatically respond (deemed as self-healing) to any failure by bringing additional capacity, where required, on-line. Finally, tier four data centres have sufficient capacity to meets the needs of the site even when redundant components or distribution paths are removed from service.

Appendix B



AQ900

Automatic fire protection system
for hazardous areas and other special risks.

Description

The AQ900 is a fully automatic fire suppression and protection system.

The unique design of the AQ900 allows the storage cylinder to be specified for either vertical or horizontal installation.

Features

"compact and effective"

Cylinder storage up to 100 litres.
Water misting, with optional additives.
Fully automatic or remote operation
Easy to install

Technical

A range of nozzle types is available including air aspirated foam nozzles as pictured here.

Smoke, heat, flame detectors, heat trace cable, or manual push button or break glass to operate.

Applications

Hazardous locations within buildings where the risk of fire is high.
Electrical rooms, transformer stations.
Engine compartments, test cells, hazardous stores, machine centers.

Fact file
Confined spaces, storage areas, engine rooms and special risk applications

Costs
Low

Further information
Tel.
+44 (0)121 693 6888
Fax
+44 (0)121 430 6007
E-mail
mail@autoquench.co.uk

Internet sites
www.autoquench.co.uk

STOP THAT FIRE

We have a policy of continuous improvement and reserve the right to change the specification at any time.
Autoquench Ltd, Priory House, 132 Priory Road, Hall Green, Birmingham, B28 0TB, England
www.autoquench.co.uk

AQ900-1b

Appendix C

Four Layer Campus Network Schematic

DIAGRAM REMOVED

Picture Courtesy of Enterasys Limited

Appendix D

Options for dual homing servers using Aggregation Switches

See attached .PDF entitled “”

QUOTE REMOVED, PART NO AND DESCRIPTION REMOVED

Cost breakdown and equipment make up is as follows:

HHCT		
QTY	**Unit Sale Price**	**Total Sale price**
4	£3,800.17	£15,200.68
4	£187.39	£749.56
8	£1,825.91	£14,607.28
		£30,557.52

PSHT		
QTY	**Unit Sale Price**	**Total Sale price**
4	£8,913.02	£35,652.08
4	£3,800.17	£15,200.68
4	£187.39	£749.56
8	£1,825.91	£14,607.28
2	£712.97	£1,425.94
4	£178.24	£712.96
8	£506.71	£4,053.68
8	£967.60	£7,740.80
		£80,142.98