Paper ref:	TB (09/18) 011

Sandwell and West Birmingham Hospitals NHS
NHS Trust

Report Title	IT Resilience and Resolution – Progress Update		
Sponsoring Executive	Rachel Barlow, Chief Operating Officer		
Report Author	Mark Reynolds, Chief Informatics Officer Toby Lewis, Chief Executive		
Meeting	Trust Board	**Date**	6th September 2018

1. Suggested discussion points *[two or three issues you consider the Trust Board should focus on]*

The Board agreed at its August meeting a programme of work to start to improve IT performance and be ready for Unity deployment (which had been earmarked for October 2018). This programme is not yet programme planned or secured but this should be achieved by September 7th. The "logicalis" element of the plan will be deployed by the November Trust Board meeting.

Since the Board met N3 connectivity has been improved after repeat failure, and a significant change has been made to our servers, again in response to failures which impacted performance. As that implies anticipatory management disciplines remain ill complied with.

Digital Infrastructure: The plan (at appendix 1) is a consolidation of previous papers on improving IT resilience. It should be read in concert with the paper provided. The document will be maintained as the overarching guide to digital infrastructure works over the lifetime of the programme.

2. Alignment to 2020 Vision *[indicate with an 'X' which Plan this paper supports]*

Safety Plan	**X**	Public Health Plan		People Plan & Education Plan	
Quality Plan		Research and Development		Estates Plan	
Financial Plan	**X**	Digital Plan	**X**	Other *[specify in the paper]*	

3. Previous consideration *[where has this paper been previously discussed?]*

Executive Group and Clinical Leadership Executive

4. Recommendation(s)

The Trust Board is asked to:

a.	NOTE the commitment to implement the agreed plan and work done to date
b.	REQUIRE the Chief Executive to complete 18-19 budget work by September 20th
c.	REQUIRE that the executive develops its 'future state model' for IT for November Board

5. Impact *[indicate with an 'X' which governance initiatives this matter relates to and where shown elaborate]*

Trust Risk Register	X	Risk Number(s): 221, 325, 2642, 3109, 3110						
Board Assurance Framework	X	Risk Number(s): BAF1						
Equality Impact Assessment	Is this required?		Y		N	X	If 'Y' date completed	
Quality Impact Assessment	Is this required?		Y		N	X	If 'Y' date completed	

SANDWELL AND WEST BIRMINGHAM HOSPITALS NHS TRUST

IT Resilience and Resolution – Progress Update

1. Infrastructure Review

Logicalis have completed their inspection of Sandwell and the retained estate at City. They aim to finish the audit by inspecting Rowley and the other Trust community sites. The supplier has yet to confirm the date for the final report but has stated verbally that no additional issues have been found.

A planning workshop was held on the 20th August where it was identified that 5 weekends will be required to undertake the disruptive elements of the remediation plan. The Trust is waiting on Logicalis to confirm when their engineers are able to undertake the works with the expectation set that this should be done during September and October.

A workshop is planned for the 7th September to start to develop a proposition for the City non-retained estate.

An initial conversation has been held with Logicalis around developing an outsourced proposition. The action is with them to reflect back with options which will inform the next steps.

2. Wi-Fi

As of 24th August all the access points will be attached to the walls in the retained estate across the Trust. Of these 88 are live with a technical issue stopping the others being used. This has been escalated to the supplier (HP) for resolution. Once resolved the remaining 300 access points will be activated.

The solution for non-retained estate at City will be included in the workshop on the 7th September as the Wi-Fi performance is closely coupled to network performance.

3. Systems/Applications Current State

During August the Trust has significant disruption due to issues with 4 different systems, 1 of which are now resolved. The fix for the two remaining systems is understood and being implemented by the IT team with a view that this is completed by mid-September.

A plan has started to be developed for the systems that need rapid improvement. Of these, 4 are scheduled for upgrade and discussions are in progress with other suppliers. The plan for the remaining elements will involve the following options:

- Replace with Unity
- Move to cloud service provided by supplier
- Upgrade
- Move to Azure

The benefits of the move to Azure is it extends support for old applications by an additional 2 years.

4. End User Devices

Orders were placed on the 9th August for the new PCs and laptops which permitted the supplier to place the order for the hardware. This was delayed from the previously reported date due to the need to gain approval on FY18 Informatics finances. An initial plan has been developed with the supplier showing these completely deployed by end November.

Ricoh (the managed print supplier) is due to shortly report back on a proposal to improve and extend the managed print service. This will remove old and obsolete printers from the Trust estate and so deliver a more reliable service.

5. Outsourced Model

- Performed an initial assessment of desktop as a service including seeking indicative costs from a supplier. This will inform the next steps with a view to undertaking a procurement.

6. Service Improvement

During August the team has:

- Documented a process manual which will be implemented during September.
- Extended risk management to all departmental managers with a formal session each month. Risk training for all managers will take place at the end of August.
- Improved its management and communication of significant IT issues including expanding the role of duty manager. This now reports formally at the end of each week.
- Completed consultation on changes to the on-call arrangements. A senior manager will be on-call from September.
- Completed a workforce skills assessment & published a training plan for staff.

Some of the work has been deferred into September due to competing pressures.

7. IT Incidents & Proactive Alerts

Performance in August has not improved as expected due to 2 weeks with significant IT issues. Improvement overall is dependent upon addressing the causes of recurrent failures. The plan remains to:

- Reduce call wait time by reducing the number of calls overall, i.e. by completing the works described elsewhere in this document.
- Reducing the backlog of incidents in the same way.
- Specific actions to resolve the critical alerts undertaken by the third line team.

Category	August 2018	July 2018	Target	Planned Date
Open incidents	808	875	400	31/03/2019
Oldest outstanding incident	December 2016	December 2016	21 days	31/03/2019
Average call wait	1m 39s	1m 11s	10s	30/09/2019
Critical alerts	49	52	0	MPA challenged a date of 31/8 and this is being reset and will be advised at the next MPA
Days since last outage	2	2	70	30/12/2018

Annex A – End User Devices & Infrastructure Scorecard

The table below describes the maturity of the IT infrastructure. The categories are:

Planned	There is a funded plan to maintain the capability including management of capacity. It includes future requirements, growth, funding and resources.
Healthy	The capability runs without issue. It means a report with no red flags (e.g. a health check report from a tool and no P1 or P2 incidents in the last period). It includes operating within capacity.
Resilient	There is alternative infrastructure to maintain the 99.9% availability SLA. This means an agreed architecture and conformance to it.
Secure	The capability meets the Cyber Security Essentials standard with no incidents.
Managed	The capability is actively monitored and managed by either Informatics or a third party

These apply to the following areas:

- **Devices** - PCs, laptops, etc, used by staff. For context, the Trust has ~ 6,000 devices
- **Mobile Devices** – mobile phones, smartphones. These are differentiated from devices in being mobile and normally come from a phone company.
- **Compute** – Large computers than run IT applications. These are also called servers. The Trust has 331 servers.
- **Databases** – A piece of software that runs on the servers. The place structured information is managed. The Trust has ~ 100 databases.
- **Storage** – Where information is permanently stored. This is either in a large array of disks or in the cloud.
- **LAN** – the internal cabled network that connects PCs to each other.
- **Wi-Fi** – the internal wireless network that connects laptops and mobile devices to each other wirelessly.
- **WAN** – the external cabled network that connects Trust sites to each other and the outside world. This is provided by N3 and companies such as BT and Virgin.
- **Print** – printers. The Trust operates ~ 1,000 printers including a contract with Ricoh for multi-functional devices (printer/photocopier/scanner).
- **Backup** – computers that take a copy of data so that it can be restored if corrupted or destroyed. The Trust backs up the equivalent of 18,000 DVDs of information.
- **Data Centre** – computer rooms. These tend to be air conditioned and may come with fire suppression.
- **Cloud –** IT infrastructure provided by someone else.
- **Telecoms –** phones, the bleep and switchboard.

Each category is then assessed against the following ratings:

Green	The criterion specified for the category is met
Amber	There are issues identified that do not have a significant impact on clinical services.
Red	There are significant issue that are having an impact upon clinical services. The criterion for the category is not met

Changes since Last Period

- **Backup** has improved as a result of implementing the new backup system. Further work is required to address 3 systems that would not backup and add additional resilience to the solution using Azure.

- **LAN** health has moved to amber reflecting that the Logicalis review found no significant issues affecting health but did recommend improvements to resilience and management.

- **Data centre** resilience has moved to red as the Sandwell data centre air conditioning has experienced another failure. The replacement purchase order has been approved by the CEO and is now being scheduled by Estates.

Area	Planned	Healthy	Resilient	Secure	Managed
End User Devices					
Devices	G	R	A	A	G
Mobile Devices	G	R	G	A	A
Printers	G	A	G	G	A
Infrastructure					
Compute	G	R	G	A	A
Databases	A	G	G	G	A
Storage	G	A	A	G	A
LAN	G	A	R	G	R
Wi-Fi	G	A	G	G	A
WAN	A	A	G	A	A
Print	A	A	G	G	R
Backup	G	A	G	G	G
Data Centre	G	G	R	G	G
Cloud	G	G	G	A	A
Telecoms	G	A	G	G	G

Annex B - IT Systems Failures

System	Clinical Area	End of Life	Week Commencing											Notes
			14/06/2018	21/06/2018	28/06/2018	02/07/2018	09/07/2018	16/07/2018	23/07/2018	30/07/2018	06/08/2018	13/08/2018	20/08/2018	
Cath Lab PC	Cardiology	Extended Support		R	R	A	A	A	A	A	A	A	G	
Merge PACS	Imaging	Extended Support			R		G							
iCM	All	Yes			R		A							DXC to submit plan to virtualise iPM (order approved)
Patient First Web	ED	Extended Support					A			A				Recurring failure to Patient First web access only
CDA	All	No		R			G							
Rhapsody	All	No		R	R			G						
JAC	Pharmacy	No	R	G				G						
Hyper-V Cluster 1	All	No					R	G			R	R	A	Follow instructions given by Microsoft with respect to updates
Connect	All	No			R			G						
Bleep	All	No			G									
Domain Controller	All	No	R	R	G					R	R	R	A	1. Amend Al Fresco to use multiple DCs for authentication. 2. Replace domain controller
Mckesson	Cardiology	Extended Support	G											
Optos	BMEC	Extended Support	R					G						
Spectralis	BMEC	Extended Support	G											
Abbott Analysers	Pathology	No						G						
Alfresco	Case Notes	No							R	G		A	A	Review Al Fresco health with Synapse
Menumark	Wards	Extended Support								G				
Information Reports	Information	Extended Support								G				
BMEC Network	BMEC	No									A	A	A	Power failure. Estates to install additional power.
Bloxx Web Browsing	Cross-Trust	Yes									G			Bloxx stable but must be replaced asap
Direct Access	Cross-Trust	No									G			Service stable but needs additional server for resilience
N3 City	City	Extended Support									R	R	A	Fix in place. Watchful waiting.

Annex C - Improvement Plan Trajectory

Area	September	October	November	December
Leadership				
Management	• Sickness management training	• Informatics vision session		• All managers completed Accredited Manager, Single Improvement Process & risk management training
Learning	• First Learning Group • 12 month scheduled of QIHD focus points • Refreshed local induction process		• We Learn sessions	• Staff survey on learning culture
Finance & Risk Management		• Risk audit	• Additional finance training for managers	
Customer Service				
Service Management	• Confirm service owners and gold/silver/bronze rating • Perform helpdesk call audit • ITIL procedure manual	• Train Service Desk in customer service • Online statistics	• Communicate issue resolution routes to Trust • IT outreach sessions	
Comms & Engagement	• Review effectiveness of comms • Document engagement plan	• Consult on and seek approval for engagement plan	• Seek suggestions from clinical and operational staff on how to improve communications and transparency of information.	

Supplier Management				
Support Model	• Develop Trust / Informatics commercial model	• Move procurement to Trust team (TBC)	•	•
Procurement	• Contract with suppliers for changes (if required)	• Commence procurement of desktop as a service • Commence procurement of network supplier		• Desktop contract award • Network contract award
Contracts Management	• Contracts register	Start service reviews for first gold systems		• Extend service reviews for silver systems.
Applications				
Stabilisation	• On-call manager rota • Improved monitoring and reporting of systems	• Merge 2nd line and PACS rota		• Prepare for Systems Administration rota
Unity	• Unity IT work complete			
Planned Upgrades	• Roche • VMware	• Unisoft / Adam	• Blood Trak	
Future Upgrades		• Azure assessment • Analytics platform	• Migration plan	

End User Devices				
Devices	• Replace iPads	• Asset management system • Laptop rollout	• PC rollout	
Mobile Devices		• All eligible mobile devices < 3 years old		
Printers	• Ricoh proposal reviewed			
Infrastructure				
Trust Network	• Logicalis Final Report • Network improvements (TBC – Logicalis)	• Network improvements	• Network improvements	• Handover to supplier
Wi-Fi	• Review outstanding issues on retained estate. • Approach for non-retained			
Wide Area Network	• VMB Firewall • Barracuda	•	• Plan FY19 improvements	•
Other	• Install bleep	• Commission bleep • Air conditioning (TBD)	•	•

Cyber Security				
Cyber Security	• Complete remaining review actions • Implement NCSC controls	•	• Named accounts for privileged access	• Regional SOC proposal
DS&P Toolkit		• Annual business continuity test (TBC) • Cyber security training	• Asset disposal audit	•

Infrastructure Plan

Appendix 1

Summary

The performance of technology in the Trust falls short of what staff should expect. In 2014 an investment programme was created, which was designed, among other gains, to have the Trust ready for EPR deployment in 2017. The present instability of our technology has resulted in a risk to 2018 EPR deployment. At the same time, the investments required both to purchase IT and to roll it out exceed the budget available. And initial analysis of the skills within the IT function suggest that we do not have the capacity nor capability to deliver the extant programme, still less adapt to more innovative digital deployments.

On the other hand, our digital maturity over the last two years has improved sharply, and we are now ranked highly alongside peer Trusts. Notwithstanding this, we would expect IT issues to form the biggest single concern raised by staff and it is understood that this requires rapid and disciplined change.

Strategic Context

The demands on technology are changing as it becomes more critical to delivering improvement in health and care. Nationally the aims are grouped within the following domains.

Within the Trust, IT must support a rich range of clinical applications from SystmOne in community to Unity across the Trust.

Governance

The Digital Infrastructure will be governed through two committees:

- Board level Digital Committee.
- CLE level Digital Committee.

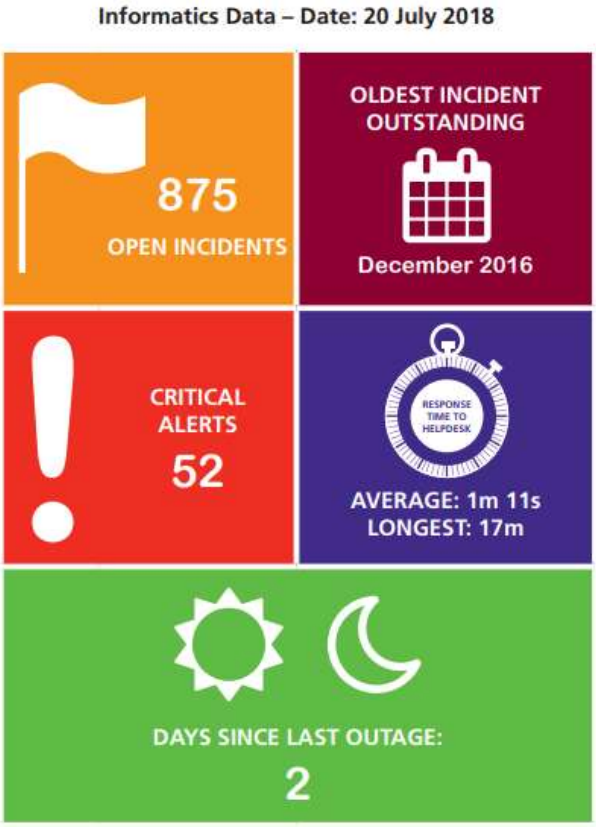
These are supported by:

- **Change Management Group (CMG) -** The change management group is responsible for the approval of changes to the IT infrastructure including new releases of applications. Downtime shall be agreed with the business through pre-approved maintenance windows or OMT.
- **Infrastructure Project Group -** The infrastructure project shall be governed by a working group. The purpose of the group is to monitor the effective delivery of the Informatics service and the status of the improvement projects. The minutes from the group shall go to the Digital Committee.
- **Technical Architecture Group (TAG) -** The technical architecture group shall be responsible for the maintenance and approval of the Trust's technical architecture.

Reporting

Progress is reported formally through the following routes:

- IT incidents are reported daily to the Executive and formally documented in a Duty manager weekly report
- Progress is reported weekly in the CEO weekly dashboard



- Monthly department progress is reported in the Informatics balanced scorecard
- IT architecture progress is reported through the Infrastructure scorecard

Area	Planned	Healthy	Resilient	Secure	Managed
End User Devices					
Devices	G	R	A	A	G
Mobile Devices	G	R	G	A	A
Printers	G	A	G	G	A
Infrastructure					
Compute	G	R	G	A	A
Databases	A	G	G	G	A
Storage	G	A	A	G	A
LAN	G	A	R	G	R
Wi-Fi	G	A	G	G	A
WAN	A	R	G	A	A
Print	A	A	G	G	R
Backup	G	A	G	G	G
Data Centre	G	G	R	G	G
Cloud	G	G	G	A	A
Telecoms	G	A	G	G	G

Our Service

Leadership

The Informatics department is developing its leadership capability internally, with the Trust and into the wider region. An internal assessment against the CQC well-led criteria identified that the department needed improvement in each category. Delivery is therefore contingent upon improving the leadership capability.

This includes better working with clinical groups including a named point of contact in the Informatics senior team.

Clinical Group	Point of Contact
Medicine	Dean Harris
Surgery	Mark Reynolds
PCCT	Martin Lynch
Imaging	Louise Brown
Pathology	Louise Brown
W&C	Sharon Reynolds

We will:

- Work together to communicate the shared Digital Plan.
- Ensure all leaders have completed the Trust's training including Accredited Manager, Single Improvement Process & risk management.
- Ensure all staff are appraised and see the role in the Digital Plan and the IT components.
- Work as a team to improve staff engagement and work/life balance with regular surveys to track progress. This explicitly includes the management of muscular-skeletal issues and stress – the two highest causes of sickness.
- Embed risk management into the department with all staff understanding how to identify, communicate and manage risk.
- Support our managers through coaching and mentoring.
- Improve financial management moving from this being reported to senior team to managed at all levels.
- Continue the investment in QIHDs with a published schedule for the next 12 months.
- Develop a learning culture including ensuring all our staff have a training plan backed up by funding through the Training Needs Analysis process.
- Develop a refreshed local induction process

The changes will provide the foundations for a successful organisation.

Customer Service

Our staff are entitled to excellent customer service with a prompt response whether that's via the Service Desk, calling the Duty Manager or a direct email. Currently the experience is varied and the right method often unclear. This can be improved.

We will improve engagement by:

- Publishing an engagement plan led by the Informatics Deputy Director.
- Work with the business to improve how, what and when we communicate, especially when things have gone wrong.
- Seek suggestions from clinical and operational staff on how to improve communications and transparency of information.
- Automate processes where we can including administration of staff user accounts and password resets.
- Update our records on the owners of gold, silver and bronze systems and provide feedback to them on system performance.
- Regularly review the effectiveness of our communications.

Alongside improving engagement there needs to be improvement in the culture of customer service so that it is applied consistently. There is regular positive feedback from customers but it is on occasion let down by inconsistency.

We will:

- Train our staff in customer service gaining accreditation through the Trust's internal scheme
- Communicate the different methods of raising an issue (Service Desk, Duty Manager) throughout the Trust so they are understood.
- Measure our success based upon customer satisfaction
- Perform an audit of helpdesk calls and identify any areas of the Trust who are not using this method. Reach out to them and identify why not and resolve.
- Reduce the backlog of calls and operate within service levels.
- Conduct quarterly outreach sessions where we collect issues from each area of the Trust rather than waiting to be phoned.
- Improve how we manage issues that relate to Community sites not owned by the Trust. This shall include closer working with Modality as a partner.
- Produce and follow a manual that sets out the procedures for the department aligning with industry standards (ITIL).
- Publish statistics online and to clinical groups on current and past performance.

These actions should result in a demonstrable increase in customer satisfaction.

Supplier Management

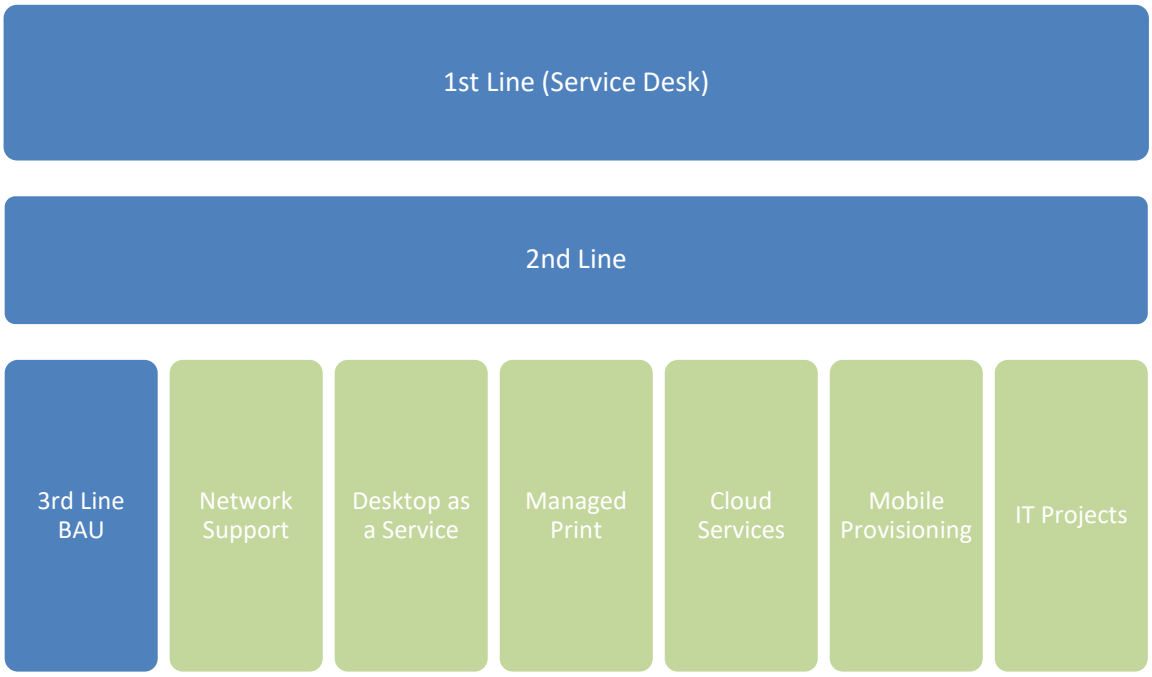
The department currently operates a model where services are provided by and dependent upon external suppliers. It manages the suppliers as procurements rather than as services that must be managed on a regular basis. Too often contracts are left to expire without renewal or suppliers are paid late.

At the moment Informatics procurement & contract management sits outwith the Trust service. The plan was always to bring it into the Trust service at the right time to undertake the mechanics of procurement, contracts management & termination. Responsibility for the service management of suppliers will remain with Informatics.

Recognising there is a lack of depth and breadth to the 2nd and 3rd line, the department will procure external suppliers to provide third line services. These will consist of:

- **Network support** – 24x7 support of the network.
- **Desktop as a service** – outsourcing of the PC hardware procurement, delivery and support. This will exclude the maintenance of the software itself.
- **Managed print** – expansion of the use of managed print.
- **Cloud services** – continuation of the use of Azure to remove the need to procure and operate server infrastructure on-premises.
- **Mobile provisioning** - reviewing the offering from EE for the provisioning, dispatch and support of mobile devices.
- **Infrastructure Project Work** – implementation of significant changes in the IT infrastructure.

This retains the 1st, 2nd and 3rd line teams to operate the remaining elements of the infrastructure in business as usual. It places a greater demand on management for the procurement and operation of the service as SWBH will be the systems integrator, i.e. responsible for co-ordinating between suppliers and holding them to account.



We will therefore:

- Consolidate all IT contracts into a single register.
- Report monthly on contracts due to expire in the next 2 months.
- Ensure that there are appropriate support contracts for our IT systems that reflect when they are used and their priority to the Trust.
- Procure network and desktop as a service providers.
- Proactively manage our gold and silver contracts through regular service reviews.
- Continue to approve IT expenditure irrespective of where the request originated.
- Work with Finance colleagues to bring IT into the Trust Procurement & Commercial service.

Applications

Stabilisation

There are a small number of systems that do not operate without issue day by day, week by week. At the time of writing these included one of the Hyper-V clusters (the main computers that run all the applications) and the City N3 link. The Trust needs stable systems it can rely on otherwise clinical care will be compromised. This is a reasonable expectation.

We will:

- Continue to follow and improve the formal change process.
- Stabilise IT services so that they run successfully over months not days.
- Ensure a Duty Manager is responsible for the Informatics service on a 24x7 basis.
- Reform IT on-call.
- Identify and resolve the underlying root causes that cause an impact on IT systems in a structured manner and report this to the Change Board. The ITIL term for this is problem management.
- Document which IT systems are used by which areas of the Trust and ensure this information is used to inform communications and engagement.
- Improve the pro-active monitoring of IT systems and reporting.

This will ensure IT systems operate reliably and that when issues are found the root cause is addressed.

Unity

After stabilising the IT infrastructure, Unity is the single biggest priority facing the department. Its implementation will draw upon staff for a number of months during the run-up to cutover, the event itself and the implementation period beyond. Unity will see a change freeze for IT work and an increase in the Service Desk staff to provide a 24x7 service.

Prior to this, Unity requires that some changes are made to IT within the Trust. Experience from other Trusts show that printing is very important as Cerner Millennium struggles to use printers connected to PCs rather to the network, hence the need for a new printing solution. There is further work to do to ensure the Cerner network connectivity is fit for purpose.

In order to support Unity we will:

- Implement a new printing solution (including new software on PCs).
- Review and improve the Cerner network connectivity into the Trust prior to go-live.
- Provide a 24x7 service for the Unity cutover.

These changes will ensure that the Trust is ready for Unity, with the printing solution required before Full Dress Rehearsal.

Planned Upgrades & Closures

The following services are either near or past the end of their useful life and need replacing. The Informatics team will work with clinical and operational colleagues to replace the following systems:

We will upgrade or replace the following IT services:

- Blood Trak (Pathology)
- Blood gas analyser (Pathology)
- Roche (Pathology)
- Viewpoint Ultrasound (Pathology)
- Telephone voice recording (Switchboard)
- Auditbase (Audiology)
- Adam (Endoscopy)
- Cleric (Patient Transport)
- BlueFish (Finance)
- Chemocare (Chemotherapy)
- VMware (Informatics)

And archive the following after Unity cutover:

- Patient First
- iCM
- Windip

This will ensure that the systems can be appropriately supported and give access to the latest functionality.

Future Upgrades

The Trust must ensure that all its applications remain current and operate on up to date infrastructure. As context:

- 110 servers use Server 2008 (R2) and must be upgraded by January 2020 or move to Azure where they are supported for another 2 years
- 181 use Server 2012 R2 and must be upgraded by October 2023

New applications also tend come with new functionality and increased reliability. This work is therefore not a one off but rather a constant task.

From a Group perspective there are 60 applications that need upgrading. These include the Gold systems PACS, RIS, Medisoft, Anglia ICE (GP orders and results)

and Telepath. The remainder are Silver and Bronze systems used within departments.

The Digital approach will be to move the services to Unity where this is available, followed by a supplier's cloud solution. Failing that the Trust will either host the software in the cloud or on premises.

We will:

- Work with departments to identify their future roadmap for the IT systems.
- Evaluate if Unity can be extended to become a suitable replacement.
- Undertake an assessment to determine which systems can be moved to the cloud.
- Create an analytics platform to support Performance & Insight.
- Upgrade our infrastructure to provide resilient cloud services.
- Upgrade or replace IT systems according to business priority, whether the infrastructure will reach its end of life and whether it is suitable for cloud.

As part of this work we will:

- Standardise the Trust's databases on a single architecture and move systems to this.
- Consolidate the Trust's information into the new storage system and turn off the old ones.

End User Devices

Devices

Traditionally the Trust has purchased devices (PCs and laptops) as and when required from capital and not managed them as an asset. Over the past 2 years there has been a significant renewal programme, replacing 3,500 PC and laptops. With just under 6,000 devices in the Trust, more need replacing each year. The Informatics department has not yet developed a robust approach to asset management needed to routinely achieve this challenge. Staff continue to report issues with PCs and laptops which correspond to a 6 year lifespan rather that the industry standard of 3 – 4 years.

The department has a maximum number of devices (5,570) based upon the licences, support, procurement and operations costs but receives frequent requests for additional devices. A review is required to determine if this is the right number and if they are allocated in the right place.

We will:

- Undertake a clinically and operationally led review of the use of devices to determine if they are optimally placed with the Trust.
- Develop an asset management system allowing traceability of physical assets.
- Replace 1,000 PCs and 140 laptops in FY19.
- Continue the rollout of laptops to Community staff including Health Visitors and Midwives. The use of iPads by Midwives will cease in readiness for Unity.
- Subject to approval, procure a supplier to provide desktops and laptops as a service.
- Ensure all devices are under 4 years old and operating on Windows 10 before Windows 7 expires in January 2020.
- Implement procedures to ensure that devices are moved by Informatics staff after an impact analysis.

This work will ensure that Trust staff have access to reliable devices using the latest operating system. Industry evidence shows that this will reduce the number of issues experienced and calls to the Service Desk.

Mobile Devices

The Trust has moved from using iPhones and iPads for staff to Android phones and only specific cases for the use of iPads. Renewal of devices has traditionally been on an as and when basis rather than a plan to keep mobile devices current. This poses challenges for reliability and cyber-security

:

We will:

- Roll out a portal to Groups so they can see mobile device spend.
- Ensure all mobile devices are less than 3 years old.
- Ensure all devices are managed via mobile device management and use this to monitor them.

This will ensure that each device is fit for purpose and secure.

Printers

The Trust printer estate has grown organically over many years and so has not been controlled or managed. There is a combination of Ricoh multi-functional devices, many of which need renewal, plus individual printers. None of the individual printers are standardised around a single model making it difficult to maintain and provide ink for them.

The department has management software for Ricoh printers but cannot see the usage on individual printers. The Ricoh data is not currently shared with Groups.

We will:

- Implement IT systems that replace patient letters with email.
- Support the move to a single letter printing provider.
- Standardise printing around multi-functional devices (MFDs) supported by individual printers in consulting rooms. Remove old printers from the estate and reduce the number of printers overall.
- Phase out the use of fax machines.
- Improve the management and reporting of printing to allow Groups to understand and control their costs.

Reducing the number of printers and standardising them will reduce operating costs and increase reliability of service for staff.

Infrastructure

Trust Network

In 2015 the Trust invested in renewing the network at City, Sandwell and community retained estate. The works was not completed at Hallam and the 3rd, 4th and 5th floor of the Sandwell main building due to issues with access. Given the new date for Midland Met investment is required for the non-retained estate.

The investment led to improvements but has not delivered a reliable service with a significant outage in May 2018. Staff report the network is slow at certain times of day. An external expert (Logicalis) has conducted a review and identified improvements to address these issues.

We will:

- Commission Logicalis to undertake the improvements they have identified. These will:
    - Amend the network to make it more resilient.
    - Upgrade the network software.
    - Improve the management capability of the network software.
    - Improve the environment (power, air, security) of the network rooms.
- Procure a supplier to operate the network on behalf of the Trust.
- Plan and then procure an upgrade for the City non-retained estate.
- Plan and then assure the implementation of networking at Midland Met.
- Implement end to end monitoring of performance so issues can be detected proactively.

This will ensure that the network has the capacity and reliability to support 24x7 services on a sustainable basis.

Wi-Fi

Good quality Wi-Fi is that covers the entire Trust is absolutely necessary to support the digital delivery of care. Clinical care requires the use of mobile devices (laptops, tablets, etc) freed from a desk, for example in taking obs or recording the patient's meal preferences. Staff report that Wi-Fi is an issue especially when using iPads in then wards. This has an impact upon clinical care.

We will:

- Replace the Wi-Fi in the hospital retained estate and Trust community buildings with a new system.
- Undertake a review by area of Wi-Fi issues to ensure they do not need an alternative resolution.
- Work with the CCGs to ensure Trust staff have access to Wi-Fi in their buildings.
- Once the new network is installed perform a survey to identify areas with poor

Wi-Fi coverage and resolve.
- Using the tools provided by the new Wi-Fi system regularly report on Wi-Fi coverage and performance.
- Procure and implement new Wi-Fi for non-retained estate (subject to financial approval)

This will ensure that Wi-Fi is not a bottleneck to using IT within the Trust and identify other issues that have been confused with Wi-Fi so they can be resolved.

Wide Area Network

The Trust wide area network allows it to communicate with the outside world. It is made up of N3 connections provided by NHS Digital and circuits procured by the Trust from BT and Virgin. There is not currently active management of their replacement and in some cases there are capacity and reliability issues. The Trust is part of an aggregated procurement to replace N3 circuits with the Health & Social Care Network (HSCN) but this will not deliver until 2019.

What we will do:

- Improve our network capability by using internet proxy filtering (Barracuda) and a new Internet connection.
- Implement resilient Internet access at Sandwell & City to remove the dependency on N3.
- Move smaller community sites (less than 10 users) to standard Internet connections where we operate the IT service.
- Work with the Clinical Support Unit (CSU) to resolve issues in community locations where the IT service is operated by them.
- Work with NHS Digital to replace N3 with HSCN.
- Procure a single network provider for all other circuits who will operate them as a single network.

This will address any issues with capacity in the wide area network and simplify the commercial management of suppliers.

Other

We will:

- Replace the air conditioning units at the Sandwell Data Centre.
- Replace the bleep.

These tasks are necessary to ensure the continued service of the infrastructure.

Cyber Security

Over the past two years the Trust has made substantial improvements in cyber security:

- Implemented patching of PC and servers.
- Moved to a new anti-virus system.
- Greatly restricted administrator access to key personnel.
- Implemented process controls and monitoring including working with the National Security Operations Centre.
- Implemented Microsoft Advanced Threat Protection on Windows 10 PCs.
- Undertaken 3 cyber security audits.

Cyber security must remain a key priority as the threat continues to evolve.

Cyber Security Improvements

We will:

- Continue to put cyber security as the number 1 priority for the department.
- Conduct annual external reviews and resolve the actions that result from them. This should include looking at advanced audits such as CREST.
- Continue to respond to the alerts, advice and guidance from the National Security Operations Centre.
- Apply National Cyber Security Centre best practice controls to the infrastructure.
- Improve monitoring and proactive testing internally on a regular basis.
- Develop a proposal for a Regional Security Operations Centre across the Black Country supported by NHS Digital.
- Ensure that only named accounts have privileged access to IT.

Data Security & Protection Toolkit

The Information Governance Toolkit has been replaced by the Data Security & Protection (DS&P) Toolkit in 2018. The new toolkit has a greater focus on cyber security and aligns with GDPR. The new focus means that Informatics must work more closely with Governance to ensure compliance.

In order to comply with the new Data Security & Protection Toolkit we will:

- Conduct an annual business continuity test that focuses on cyber security
- Fully document systems information flows.
- Regularly review our IT systems list to ensure GPDR compliance, whether it contains personal identifiable data and if there is an appropriate level of user authentication.
- Embed data protection by design including the use of Data Protection Impact

Assessments.

- Undertake a review of the PC destruction certificates in last 12 months led by Governance.
- Ensure all Informatics staff complete Cyber Security training.
- Validate that all network equipment has had its default password changed.
- Check external web applications again the OWASP standards.
- Document the processes by which data can be extracted from systems to support data portability requests.

The actions will improve the Trust's overall security and ensure compliance with policy & Law.