Brent	**Joint Committee of the London Boroughs of Brent, Lewisham and Southwark** 2 March 2021
	Report from the Managing Director of Shared Technology Service

Shared Technology Services Update

Wards Affected:	N/A
Key or Non-Key Decision:	N/A
Open or Part/Fully Exempt: (If exempt, please highlight relevant paragraph of Part 1, Schedule 12A of 1972 Local Government Act)	N/A
No. of Appendices:	Four Appendix A: Shared Technology Services Performance Pack Appendix B: Cloud Programme Update Appendix C: Shared Technology Technical Roadmap Executive version Appendix D: Shared Technology Services Cyber Strategy
Background Papers:	None
Contact Officer(s): (Name, Title, Contact Details)	Fabio Negro Managing Director of Shared ICT Services Fabio.Negro@brent.gov.uk

1. Purpose of the Report

1.1 This report provides an update on Shared Technology Services (STS).

2. Recommendation(s)

2.1 The STS Joint Committee is asked to:

a) Note the actions being taken in Section 3 – Detail

b) Note the contents of the Performance Pack as attached in Appendix A

3. Detail

Summary

3.1 During the four-month period, October and November saw similar call volumes of just over 8,000 calls each month in STS queues. As expected, call volumes dropped in December to 6,393 due to the Christmas break and this allowed us to reduce open call numbers. In January call numbers have risen back to pre-Christmas levels.

3.2 A Shared Technology Service Cyber Strategy was created to outline our approach in defending the residents and council data. The Strategy has been included in Appendix D.

3.3 In the last quarter, good progress has been made with the Continuous Service Improvement Plan activities and a further 10 activities are now closed down.

3.4 The production of the Technology Roadmap has been produced please see Appendix C for further detail.

3.5 As a result of centralising the management of audits it has highlighted how many STS have been managing which total 15 Audits, which compromises of:

- 7 reports that have final reports and recommendations and are being tracked. STS have completed most of the management actions see table below for more detail
- 2 legacy audits from 2018/19 for Lewisham and Southwark and all management actions have been completed
- 6 audits for 20/21 that are in varying stages between scoping and receiving final reports with recommendations and management actions.

3.6 The Target Operating Model was approved by Joint Committee on 18th January.

3.7 We are now in a 30-day period of consultation with the staff members on the proposed restructure, which was initiated on Monday 8th February.

3.8 The Shared Technology Service (STS) is forecasting an underspend of £2,418 for 2020-21, against a total budget of £14,477,314. The underspend is primarily due to investment cases covering identified revenue pressures.

Service Performance

3.9 The shared service logged 45,407 tickets between 1st October 2020 and 31st January 2021 (an average of 11,350 tickets per month) against 36,658 in last period, July to September 2020 (an average of 12,220 tickets per month), these tickets consisted of both issues and service requests.

This is broken down by (previous period numbers in parentheses):

- Shared ICT Services – 28,982 - an average 7,245 per month (24,780 - an average of 8,260 per month)
- Brent Applications Teams – 8,562 - an average of 2,140 per month (6,695 - an average of 2,231 per month)
- Lewisham Applications Teams – 3,687 - an average of 921 per month - (2,854 - an average of 951 per month)
- Southwark Application Teams – 1,452 - an average of 363 per month (1,426 - an average of 475 per month)
- Other customers (e.g. LGA) – 2,724 - an average of 681 per month (903 - an average of 301 per month)

3.10 Since the Joint Committee last met (4 months), there have been 14 priority 1 incidents within STS queues, of which 7 were resolved within the service level agreement. There were also 3 non-STS related P1s. This is an increase over the previous period and more detail can be seen in the performance pack – but 7 of the calls were related to the public web sites of Lewisham and Southwark councils. There were three main infrastructure-related failures, but these centred around ageing components that will be due for decommission, replacement or upgrade in the coming year. The shared service continues to focus on infrastructure and process improvements in this area to reduce these numbers.

3.11 During the four-month period, October and November saw similar call volumes of just over 8,000 calls each month in STS queues. As expected, call volumes dropped in December to 6,393 due to the Christmas break and this allowed us to reduce open call numbers. In January call numbers have risen back to pre-Christmas levels.

3.12 The number of priority 1 incidents increased in this reporting period, mainly due to multiple issues with the public web sites of Lewisham and Southwark councils. There were three main infrastructure-related failures but centred around ageing components that will be due for decommission, replacement or upgrade in the coming year.

3.13 Priority 2 and 3 issues within STS queues have seen an average of 72% and 71% compliance with the service level agreements (against 57% and 64% reported for the previous period). STS has placed considerable emphasis on improved call management and that can be seen in the improved SLA performance. STS will continue to work to improve the service levels.

3.14 The Joint Committee had requested further detail as to the categorisation of the P2 and P3 calls. The development of additional monitoring tools in PowerBI has allowed us to identify areas of focus.

3.15 The top six categories for P2 calls (69) logged in STS Hornbill queues during October to January are as follows:

Category	Number of Calls
Server Issues	20
Software/Firmware	8
Network Issues	5
Application database	5
Telephony	4
Service password issues	2

3.16 The top six categories for P3 calls (only the first 10,000 can be analysed in Hornbill, but total was 10,316) logged in STS Hornbill queues during October to January are as follows:

Category	Number of Calls
Advice/Training given	2453
Software/Firmware	1007
Folder/File issues	506
Password Reset	391
Hardware	357
Restart/reboot	151

3.17 Priority 4 service requests within SICTS queues for this reporting period have an 80% compliance with the service level agreements (compared with 78% for the previous reporting period).

3.18 The shared service operated a programme (Call Biltz) to reduce the number of open/on-hold tickets within Hornbill. At the height of the first Covid-19 wave, the shared services open/on-hold queue had over 4,500 tickets, but over the Christmas period we were able to reach the target of 1,500. Since then, due to demand in January, the count now stands at approximately 2,400 but this is still a considerable reduction on the original total. With the STS restructure imminent, we expect to be able to reduce numbers further. The impact of this, and of improved call handling and management processes that have been instigated, has led to improved SLA performance.

3.19 Net Promoter score is an industry standard for monitoring the experience of our service. Anything above zero is considered to be good, with above 50% ranked as excellent. In this reporting period we have been able to achieve over 60% - this is detailed in the accompanying performance pack.

3.20 Hornbill, our customer portal, is being developed to present a more user-centric experience which should lead to better categorisation of calls being logged. This in turn should allow us to introduce more automated workflows to speed allocation and resolution of incidents and request tickets. A trial of the new experience has been taking place in the partners with positive feedback.

3.21 Due to the much greater requirement for remote/home working and to support the new backup system (which uses cloud-based storage), the Internet link bandwidth in the STS datacentres is being upgraded from 1Gb to 10Gb. The

STS Croydon datacentre link was upgraded in January with the STS Brent datacentre link to be upgraded in March. This will also mean that we have enough bandwidth to cope with all connections should one of the links fail. It will also allow us to consolidate Southwark Council's Internet links when the existing contract for those circuits ends in 2022.

3.22 The telephone support line which was introduced at the start of the Covid-19 situation has been maintained and while popular, the engineer resource requirement for this has placed a pressure on the service desk, and response times have increased.

3.23 The out of hours support telephone service (introduced in March 2020), is backed up by a third-party and has proved successful. As part of the restructure and new target operating model, it is intended to extend that service to 24x7x365 through a third-party, to provide a more responsive telephone service for urgent/time-sensitive support calls where the Hornbill Portal may not provide the timeliest resolution – this will take the place of the in-hours telephone service currently provided (please see previous point). This service will additional capacity to the telephone lines (and there will be an agreed SLA answer time for any telephone calls into the service desk) plus this will free up engineer resources on the service desk to attend to other calls.

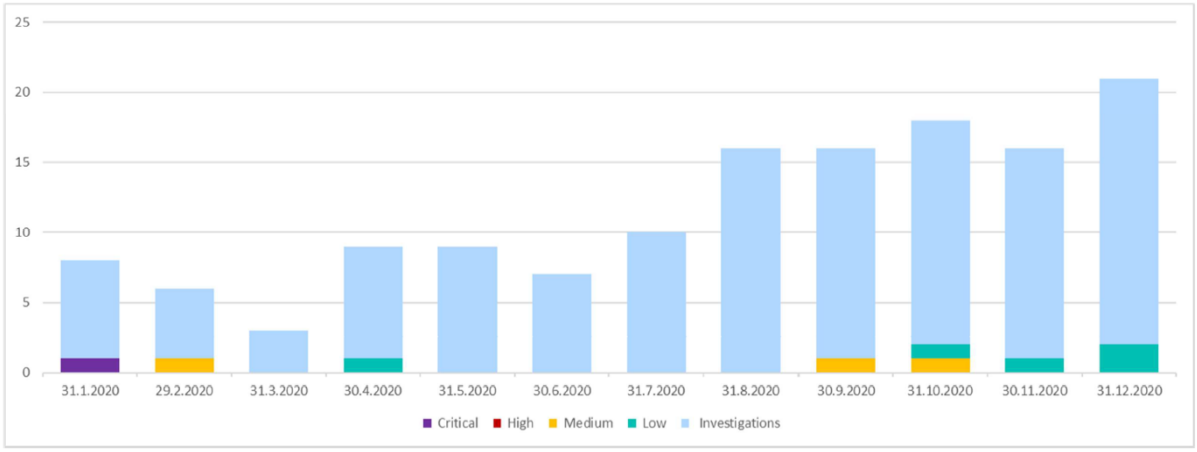
It is anticipated this service will be operational by April 1st 2021. STS will operate an out of hours P1 escalation service to manage any major incidents that may occur outside of core hours.

Cyber Security

3.24 During this last period, we have not had any serious cyber security issues, we continue to work with a third party recommended by the National Cyber Security Centre to proactively monitor our environment.

3.25 As we continue to harden our infrastructure, we see a continuing reduction in security incidents over the past 12 months. Other than false positives, no incidents have been raised in this period by our threat protection partner.

Initial investigations take place when anomalies are spotted such as vulnerability scans or out of the ordinary AD Sync actions. In some cases, these are closed before contacting shared service in others we may be asked to confirm that an action is known about and expected. Both the lows show here related to advice about the SolarWinds supply chain attack. The full report from F-secure can be made available.



3.26 The internal infrastructure was critically behind on some of our security controls and there has been an active programme to bring the infrastructure to acceptable levels. During the coming months there will be a continued focus on the hardening of our infrastructure. Tools have been purchased to aid both vulnerability management and patching across the server estate, to be deployed by end of March 2021.

3.27 Much work has taken place both with MHCLG and the LGA in response to several high-profile cyber-attacks. Responding to surveys covering the following areas of cyber security.

- Identify
- Protect
- Detect
- Respond
- Recover

Initial focus for the shared service has been on the respond and recover given the importance of offline backups in the case of a ransomware incident.

A decision was taken to bring forward the procurement and installation of a new backup system to ensure the security and integrity of the backup data as well as enhanced recovery capability in the event of an attack such as Ransomware. A Rubrik backup solution has been procured and it is expected to be fully installed and configured by the end of March this year. This will give us both short term (14 days) on-premises backup storage (in the form of a backup appliance that has an immutable file system and multi-person/multi-factor authentication for any administrative action that could modify or delete backed-up data) and Azure cloud storage (replicated between multiple Azure datacentres) for longer term (13 months) backup storage. This configuration complies with NCSC guidelines for a secure backup solution. Work is ongoing with MHCLG to obtain funding for projects related to the ongoing ransomware remediation effort

3.28 Public Service Network (PSN) compliance allows the councils to connect to other government networks such as the NHS and DWP. Brent is currently compliant,

Lewisham has resubmitted with updates in February and Southwark have had a health check and a submission is being prepared.

3.29 Payment Card Industry (PCI) is the accreditation required to allow organisations to take electronic payments such as those we have on the website and in Libraries. This only applies if the council manage the payment service. Brent and Lewisham are both currently accredited. Southwark outsource its payment service therefore not applicable.

3.30 Brent and Lewisham have an old smartphone estate which is being scheduled for upgrade. These devices are falling below current security compliance levels. Brent have started a replacement programme and are near to completion. Lewisham are considering its model around mobile telephony and strategy is currently being developed. Southwark have very few outstanding devices and are being managed on a case-by-case basis.

3.31 A considerable amount of work has gone into managing numbers of accounts across the three councils. A review of the starters, movers and leavers process has been completed to ensure that we have as few enabled accounts as possible. This limits the possibility of them being exploited and is also important due to licencing and the costs surrounding that.

3.32 We have seen 15.3 million emails attempt to reach the councils within a 30-day period. Over 85% of these emails were stopped because they were spam or malicious email such as ransomware. The layers of protection have ensured that the councils have avoided serious incidents.

3.33 A Shared Technology Service Cyber Strategy was created to outline our approach in defending the residents and council data. The Strategy has been included in Appendix D.

Continuous Service Improvement Plan

3.34 In the last quarter, good progress has been made with the activities and a further 10 activities are now closed down.

3.35 To continue with this good progress, the STS Senior Leadership Team have been reviewing progress of the CSIP every month, and quarterly reviews are scheduled with the Operational Management Group.

3.36 There have been no tasks added to the plan in the last quarter and there are 16 tasks remaining on the plan, 10 of which are in progress and the remainder scheduled to commence after implementation of the new Target Operating Model organisational structure, when dedicated resources for Service Design and Improvement are expected to take ownership of the plan and any additional items.

3.37 This team will be tasked with identifying and prioritising further service improvement opportunities such as continuous improvement to our portal, development of a detailed Service Catalogue, and improving our overall processes, data quality & reporting.

3.38 The current plan to improve our service is based on the categories below:

- Strategy & Governance
- Network & Communications
- Infrastructure
- Finance & Procurement
- Enterprise Support
- Customer Experience
- Service Desk

3.39 The launch of a redesigned portal, originally planned for Q4 2020, has been deferred until late Q1 2021 after assessing after assessing some operational issues. When launched, we expect this portal to improve the categorisation of user reported issues as well as the subsequent handling and reporting; the ultimate aim being to reduce the average time to resolution.

Audits

3.40 Since the last Joint Committee in October 2020 all audits are now managed centrally by the Head of Service and are reviewed monthly by STS senior leadership team to ensure that recommendations and management actions are tracked through to completion.

3.41 As a result of centralising the management of audits it has highlighted how many STS have been managing which total 15 Audits, which compromises of:

- 7 reports that have final reports and recommendations and are being tracked. STS have completed most of the management actions see table below for more detail
- 2 legacy audits from 2018/19 for Lewisham and Southwark and all management actions have been completed
- 6 audits for 20/21 that are in varying stages between scoping and receiving final reports with recommendations and management actions:

  - Brent – **IT Asset Management Review**
  - Brent – **IT Project Review**
  - Lewisham - **Smart tech roll out project**
  - **L**ewisham - **Cyber – Remote working arrangements**
  - Southwark – **Mobile phone management**
  - Southwark – **Asset Management**

3.42 STS have met with the borough IT Directors and audit departments and are working collaboratively to agree 21/22 audits plans. Plans will be shared at the next Joint Committee once they have been agreed.

Brent - IT Sourcing Audit This audit is to assess the design and operating effectiveness of the IT sourcing.		
Create third Party Data Register	Medium	Completed

Service Level Agreement (SLA) Strategy and Performance Monitoring (Contract Monitoring)	Medium	Completed
Business Continuity Management (BCM) and Disaster Recovery (DR)	Medium	Completed
Third Party Risk Management Framework / IT Procurement Policy	Medium	Completed
Central Repository & Register for Contracts	Low	Completed

Brent - IT Governance Audit This audit is to ensure that appropriate financial, decision-making and portfolio management structures are in place so that IT can enable the Council to deliver on its objectives and mandate.		
Introduction of SLA Penalties	Medium	Completed
Creating a single risk register for the SICTS	Medium	Completed
EOS (end of support) and EOL (end of life) IT Infrastructure	Medium	Completed
Introduction of IT Organisational Chart	Low	Completed

Brent - IT Platform Governance review This audit is to ensure that IT platforms (Microsoft Windows) have appropriate governance, operational and security controls and that the security configurations are maintained and kept updated.		
Authorised staff members can make changes	High	Completed
Monitoring of user activity	High	Completed
User access review	Medium	Completed
Platform Policies / Standard Operating Procedures	Medium	Completed
Unsupported Operating Systems	Low	Completed

Brent - IT Disaster Recovery The objective of this review is to evaluate the design of the Shared Service's IT DR planning framework and processes to assess whether they are appropriate, complete and robust, and to explore whether there is sufficient assurance that the arrangements will operate in practice.		
Failure to periodically test the IT DR plan can result in the systems not being recovered within required recovery time objectives should the need for DR be invoked.	High	In progress
If the ITDR capability is not overseen by an appropriate organisational structure representing all business services at an effective level, there is a risk that it will not meet business recovery requirements.	Medium	In progress
Failure to ensure that the DR plan is updated regularly especially after significant changes in the business or ICT environments can result in misalignment between achievable recovery times of key systems, not meeting	Medium	In progress

the objectives and expectations of the Council to deliver its services.		
If the criticality of systems is not established and reviewed on a regular basis, or as soon as the system is implemented, and taking account of all Council business systems, it may mean the correct level of risk is not associated with it failing and impact the priority of recovery action taken in the event of disaster.	Medium	In progress
The recovery of the applications and services in scope may be delayed if supporting interfaces and dependent systems are not defined and the recovery tested simultaneously. This could result in failure to deliver critical services within the agreed timeframes.	Medium	In progress
Lack of established and defined procurement third party risk assessment processes may lead to business disruption at the supplier not being effectively flagged and resolved. This may have an adverse impact on Council operations.	Medium	In progress
If an incident is replicated at both sites this effectively removes any option to failover to a known safe state and environment. The only option remaining would be to rebuild and restore services from a network-isolated backup copy. If restoration is not pre-planned, and the restoration time known, the resulting business impact is likely to be adverse.	Medium	In progress
Staff may receive insufficient training or may not be made aware of IT DR arrangements and their role within them, which may result in an ineffective response.	Medium	In progress

Lewisham - Telecommunications Audit This audit focuses on resilience, system security, application governance of the telephony system.		
System Security – Administrator Access	Medium	Completed
System Security – Monitoring of Unsuccessful Logins	Medium	Completed
System Security – Generic Phone Handset and Voicemail Passwords	Medium	Completed
System Security – Generic Phone Handset and Voicemail Passwords	Medium	Completed
Disaster Recovery and Maintenance – Disaster Recovery Arrangement	Medium	Completed
Resilience, Disaster Recovery and Maintenance – 3rd Party Assurance over the 8x8 Network	Medium	Completed
Application Management and Governance – Telephony Asset Management	Low	Completed
Application Management and Governance – User Management	Low	Completed
System Security – Monitoring of Remote Access Ports	Low	Completed
System Security – Security Policy	Low	Completed

System Security – Automated Switchboard Maintenance	Low	Completed
System Security – Reverse Charge Calls	Low	Completed
Call Restrictions – Call Barring and Restrictions	Low	Completed
Resilience, Disaster Recovery and Maintenance – Switch Configuration Backups	Low	Completed
System Monitoring Reports and Value for Money (VFM) – Call Logging	Low	Completed
System Monitoring Reports and Value for Money (VFM) – Telephone Bill Reconciliation	Low	Completed

Southwark - Website Security and Maintenance This audit appraised the design and operational effectiveness of the Council's procedures for identifying and protecting its website and for managing the security and maintenance risks on an ongoing basis.		
Resilience and continuity arrangements for wed application may not be adequate to ensure timely recovery following an attack	High	Completed
Patch management, change control and antivirus for the website is ineffective and lead to outdated services, unauthorised changes and unprotected servers	Medium	Completed
Resilience and continuity arrangements for web applications may not be adequate to ensure timely recovery following an attack	Medium	Completed
Vulnerability scanning and remediation of web servers and applications is ineffective and leads to critical vulnerabilities not being resolved	Medium	Completed
Patch management, change control and antivirus for the website is ineffective and lead to outdated services, unauthorised changes and unprotected servers	Low	Completed
Policies and procedures for website maintenance and administration may not be up to date, or understood and followed by administrators	Low	Completed
Patch management, change control and antivirus for the website is ineffective and lead to outdated services, unauthorised changes and unprotected servers	Low	Completed

Southwark - Shared ICT Review This Audit focuses on governance and performance issue resolution and future planning.		
As a result, there is a risk that the resolution of the major incidents are not within the SLA target. Furthermore, there is a risk of any tasks assigned in a meeting may not address the root cause of the issues discussed and that trends may not be identified for categorisation of the issues.	Medium	Completed

As a result, there is a risk that the IAA may not provide the councils with the updated level of service they require	Low	Completed

Where audits have all actions complete, they will be removed from future Joint Committee reports.

Road Map

3.43 The production of the technology roadmap has been produced please see Appendix C for further detail.

3.44 The technology road map is now being enacted and we have added estimated timescales for Business Cases to be written and approved, so that we are able to keep to planned spend each year.

3.45 For the identified 5 technology themes, the top-level capital investment projections for 5 years are as follows:

1. Data Centre Improvements: £11m
2. Campus Networking Refresh: £4m
3. End User Experience Modernisation: £12m
4. Cyber Protection: £4m
5. Service Improvement: £1m

3.46 The IT roadmap will be integral for the design of the future target operating model and has been developed in tandem with this. For example, the roadmap highlights the potential need for several project resources to deliver the technology changes.

3.47 A draft Executive Summary of the key elements in the roadmap has now been written and distributed for comment.

Target Operating Model

3.48 The Target Operating Model was approved by Joint Committee on 18th January.

3.49 We are now in a 30-day period of consultation with the staff members on the proposed restructure, which was initiated on Monday 8th February.

3.50 After consultation has been completed, the team structure will be finalised, and all vacancies will be advertised internally to the team initially.

3.51 Following this internal recruitment round, remaining vacancies will then be advertised to partner councils and externally. We have initiated four workstreams to progress with this recruitment:

1. Talent Acquisition – Executive search, digital marketing across multiple channels, LinkedIn recruitment.
2. Internal Process – Selection & interview process, internal communications and reporting.
3. Up skilling – Training needs analysis for new placements.

4. Engagement – Defining candidate journey & onboarding in the current remote working environment.

3.52 Our target implementation date for the new structure is 10th May 2021, subject to successful recruitment, selection and onboarding of new colleagues.

Lewisham Homes

3.53 STS and Lewisham Council have produced a report for the provision of IT infrastructure support services for Lewisham Homes that was taken to and approved by the Joint Management Board.

3.54 The report recommended that the current model of apportionment will continue, and LH will be added to the Lewisham council contribution to the shared service. Governance will continue as it operates with the same membership. Lewisham Homes will be represented by Lewisham council. Lewisham Council will present its proposal (based on the report) for the model to Lewisham Homes.

3.55 "Deep-dive" discovery workshops and knowledge transfer, alongside operational alignment tasks, will take place to ensure that the migration of the Lewisham Homes datacentres to STS datacentres and the ongoing support of Lewisham Homes users will occur in a timely manner with as little risk as possible. The expected timeline for this is in June/July of this year.

3.56 It is likely that there will be TUPE implications to consider for both the shared services and for Lewisham Council.

Project Updates

3.57 STS have 61 In flight projects across Brent, Lewisham and Southwark.

3.58 To ensure that we manage the projects more effectively we meet with each borough on a monthly basis, at the project review meetings we go through the inflight projects, paying particular attention to the amber and red RAG status projects to ensure that the right focus and work collaboratively to unblock issues that may arise.

3.59 We also review all potential pipeline projects at the project review meetings, this is both STS and Council led projects, so we all have sight of what is potentially coming up stream and plan accordingly.

3.60 We are currently working on demand and capacity management tool to help with identifying where resources will be oversubscribed which will help with scheduling pipeline projects more accurately for both our own and our partner's ongoing developments.

3.61 The Cloud programme after successfully completing Foundation phase in Summer 2020 is now working only on the Southwark related work. As a result, Southwark requested taking over direct governance of the programme team, costs, and remaining workload. This work covers migration of those required business and infrastructure applications remaining in the Capita data centres

(DCs) along with secure decommissioning of this server estate.

3.62 Southwark has identified 49 business applications needing to be migrated. The programme team are now working closely with business owners to ensure these systems are still required with the migration work being managed by our Infosys (our strategic cloud partner). Migrations are underway, supported by detailed dialogue with business owners and application suppliers.

3.63 In addition, there are a total of 959 servers that must be securely decommissioned to complete the exit from Southwark's Capita DCs by September 2021.

Procurement Updates

3.64 O2 contract for Southwark: Formal documentation put together by O2 was initially unsatisfactory and did not match original pricing on which the award was based. This had to go back to O2's commercial team but is now resolved. It is expected that the agreement will be entered into by the end of February.

3.65 The MobileIron MDM contract for Brent and Lewisham has been renewed to 30 November 2021, allowing time for consolidating MDM on Microsoft InTune later in the year. When the consolidation happens, savings will be realised as the MobileIron contract will have ceased. The renewal cost was £57k.

3.66 An implementation partner for Brent's new Sitecore web content management system has been procured.

3.67 The Ricoh contract has now been varied, with the required amendments to the contract model that accommodate changes to ways of working due to Covid-19 and giving transparency of pricing that will enable savings to be identified if there are further changes in machine numbers.

3.68 A new contract for Countercept Managed Detection and Response has been procured, providing significantly increased device coverage with a slight reduction on the £170k annual cost of the previous contract. Contract is for three years (2 plus 1).

3.69 Two separate five-year contracts for the new backup solution have been procured, one for the solution itself and another for the MS Azure storage that it will require.

3.70 A new contract for ProofPoint email filtering and fraud defence has been procured, to 25/02/22.

3.71 A procurement of a new three-year contract for Forcepoint web filtering is underway.

3.72 Procurement options for the Microsoft "ramp" to E5 for Southwark re being explored. It is planned to take an award decision to Brent's Cabinet in May.

4. Financial Implications

4.1 The Shared Technology Service (STS) is forecasting an underspend of £2,418 for 2020-21, against a total budget of £14,477,314 (this excludes the £120k accrued income from 2019/20). The underspend is primarily due to investment cases covering identified revenue pressures.

4.2 The total budget of £14.48m is a combination of non-controllable expenditure of £7.75m and controllable expenditure (staffing and consultancy) of £6.73m.

4.3 STS continue to operate under the improved charging process with the consumable recharges and project costs being stripped out effectively. From April 2020 to January 2021, a total of £6.59m of recharges have been identified and accounted for. This significantly helps eliminate any budgetary pressure STS would have encountered if these costs were absorbed in the core budget.

4.4 This favourable financial position has developed due to several improved practices:

- Financial reporting – monthly budget review and charging meetings with all partners
- Clarity around licencing costs – material licences have been identified and have been built into the core 2020/21 budget
- The Microsoft settlement being finalised, and year 2 funding being made available to cover this
- Capital costs being correctly identified and treated taking away any revenue pressures

4.5 Additional funding was needed to respond to the Covid-19 situation, Brent £375,667, Lewisham £331,072 and Southwark £173,155.

5. Legal Implications

5.1 This report is for noting. Therefore, no specific legal implications arise from the report at this stage.

5.2 Brent Council hosts the Shared ICT Service, pursuant to the Local Government Act 1972, the Local Government Act 2000, the Localism Act 2011 and the Local Authorities (Arrangements for the Discharge of Functions) (England) Regulations 2012. These provisions allow one council to delegate one of its functions to another council as well as allowing two or more councils to discharge their functions jointly with the option of establishing a joint committee. Joint committees can in turn delegate functions to one or more officers of the councils concerned. Decisions of joint committees are binding on the participating councils. However, subject to the terms of the arrangement, the council retains the ability to discharge that function itself.

6. Equality Implications

6.1 During the current Covid-19 crisis, the Shared Service has always followed government and council guidelines and policy to ensure the safety of our officers. Those officers in vulnerable categories or caring for others who may be vulnerable have been working

from home at all times. We have maintained a small staff presence at the council head offices, and have provided appropriate PPE equipment along with social distancing measures at all times,

7. Consultation with Ward Members and Stakeholders

7.1 There are none.

8. Human Resources/Property Implications (if appropriate)

8.1 The Target Operating Model will indicate the need for a future restructure of the service, this will be presented with a business case by the Managing Director.

Report sign off:

PETER GADSDON
Strategic Director of Customer & Digital Services