MINUTES OF THE JOINT COMMITTEE OF THE LONDON BOROUGHS OF BRENT, LEWISHAM AND SOUTHWARK
Held in Meeting Room G01, Southwark Council, 160 Tooley Street on Tuesday 26 November 2024 at 6.00 pm

PRESENT: Councillor Stephaine Cryan (Chair) and Councillor Barrie Hargrove (London Borough of Southwark), Councillors Mili Patel and Jake Rubin (London Borough of Brent) and Councillor Amanda De Ryk (London Borough of Lewisham).

1.   **Appointment of Chair**

      RESOLVED that in accordance with Section 10 of the Joint Committee's Terms of Reference, Councillor Stephanie Cryan (as representative of the hosting Authority – London Borough of Southwark) be appointed as Chair for the duration of the meeting.

2.   **Apologies for Absence and Clarification of Alternate Members**

      An apology for absence was received from Councillor James Walsh (London Borough Lewisham).

      No other apologies were received at the meeting.

3.   **Declarations of Interest**

      There were no declarations of interest declared by Members at the meeting.

4.   **Minutes of the Previous Meeting**

      RESOLVED that the minutes of the previous meeting of the Joint Committee of the London Boroughs of Brent, Lewisham and Southwark held on Tuesday 19 March 2024 be approved as a correct record.

5.   **Provision for Public Participation**

      No deputations or requests to speak were received at the meeting.

6.   **Shared Technology Service Update Report**

      Fabio Negro (Managing Director Shared Technology Services) introduced the report to the Joint Committee providing an update on key performance areas in relation to the Shared Technology Service (STS).

      Members noted the summary of key performance management indicators for the service across all three Council's, which had been included within the report and in

terms of detailed service performance, the Joint Committee were advised of the following:

- Whilst progress continued to be made in the overall reduction of open STS operational calls, there had been an increase in the current reporting period (July – October 2024).

- In the current reporting period (July – October 24) there had been eight Priority 1 incidents related to STS infrastructure, six of which had been resolved within SLA, with six application/supplier related P1 incidents.

- P3 incidents remained the most common type of incident, as these were related to issues experienced by individual users. The target SLA was to resolve 90% of P3 incidents within two working days. 13,667 P3 incidents had been logged into STS operational queues by partner councils during this reporting period, with an overall SLA performance of 82% (compared with 87% in the previous reporting period) and the top eight categories for P3 calls detailed in section 4.8.4 of the report. This had coincided with an overall increase in demand during the reporting period, with the STS having seen around 850 calls more per month logged than in the previous reporting period and the majority of these being classified as P3 incidents.

- Priority 4 incidents were defined as requests for standard service or catalogue item. The standard SLA was to resolve 80% within 5 working days. In the current reporting period, there had been 10,137 P4 requests logged into STS operational queues, with an overall SLA performance of 90% compared with the previous reporting period figure of 93%. Whilst noting that SLA performance had dropped slightly, members recognised this has been impacted by the increased number of P3 incidents with the top call logging categories for STS operational P4 requests detailed in section 4.9.3 of the report.

- The impact of the higher level of demand on operational services, such as the upgrading of servers (Windows 2012), the rollout of Office 365 applications across the councils, emergency planning, and resilience exercises, high-level of infrastructure change and ageing laptop fleet as further context in relation to the overall level of P3 & P4 performance.

- The detailed provided within section 4.3 of the report on the number of open calls currently in STS operational queues. Whilst progress continued to be made in the overall reduction of open STS operational calls, it was noted there had been an increase during the current reporting period (July – October 2024) which reflected the demand in terms of tickets raised in STS operational queues arising from the high level of change across all three councils and change-related issues.

- The ongoing focus on the customer experience including the development of on-site and telephone support with the overall number of calls logged between July – October 24 reported as 57,889 tickets for all council application teams as well as the shared service (representing an average of 14,472 tickets per month) against 53,147 in the previous reporting period. Members were

advised the tickets consisted of both incidents and service requests with the breakdown by each authority provided within section 4.13.1 of the report.

- Whilst the last 12 months had seen an improvement in performance against key SLA KPIs, members were also advised of the following initiatives being taken forward in relation to the customer experience:
  - ➢ The trial (in one member authority) of a new on-site approach for visitors removing the requirement for on site visitors to log Hornbill calls prior to their visit.
  - ➢ The introduction of new signage in the form of a roller banner at the registration desk to guide users through the process of registering with the QMinder System and to publicise a QR Code/URL that could be accessed from mobile devices to check how many visitors were in the on-site queue and the average wait time.
  - ➢ The introduction of a scripted welcome from engineers to provide a more welcoming and consistent experience for visitors.
  - ➢ The planned introduction of an on -site reception/concierge service along with enhanced induction process for new starters with the Service Desk Telephone Support Line contract also due for renewal in April 25 and the escalation process for Hornbill calls also having been refined.

- The ongoing focus (as detailed within section 5 of the report) on continuous service improvement activity including work streams relating to user experience and assets, which had included areas such as the laptop refresh process for which the contract had now been awarded and the LGA pilot was underway with Brent to follow. Members noted the update provided on the procurement process review (as detailed in Appendix 2 of the report) with the Joint Committee advised that Southwark were now in the process of approving the business case for phase 2 of the project and Lewisham's business case currently being drafted.

- The details provided on the top 10 risks identified for the STS and the relevant mitigations in place to address them, as detailed within section 6 of the report. This had included a series of cyber security emergency planning exercises with details also provided (within Appendix 1 of the report) on the recent CrowdStrike outage, impact on servers operated by member authorities and the recovery response initiated by the STS.

- The progress being made in relation to delivery of the Technology Road Map 2026 (as detailed in section 8 of the report) along with planned development of a future IT Modernisation investment plan.

- Updates were also provided in relation to a range of other key projects, as detailed in section 9 of the report including the Windows 2012 upgrade (as detailed in section 9.4 of the report) on which work to complete necessary server upgrades across all member authorities was expected to be completed by early 2025.

- The individual digital progress updates provided within section 11 of the report, relating to Brent, Lewisham & Southwark Council's as a newly introduced element to the update report for the Joint Committee.

The Chair thanked Fabio Negro for the service performance update provided with comments then invited from Members and the following issue(s) raised:

- In terms of the growing demand identified in relation to number of tickets being logged, further details were sought on the impact in terms of call wait times and also whether details were available on calls not completed . In response, Fabio Negro confirmed that these metrics were available with an outline of performance in relation to telephone support provided within section 4.11 of the report. Members advised they would be keen for future update reports to include details on performance relating to call wait times recognising the service improvement features being sought as part of the tender renewal process for the Service Desk Telephone Support Line Service (including providing an expected wait time to be connected to an engineer), enhancement of the Hornbill call management and triage system and also anticipated increase in calls logged during the laptop refresh project.

Having considered the service performance update, the Chair than invited Fabio Negro to introduce the updated STS Strategy 2024-26 to the Joint Committee for formal approval and adoption.

In presenting the STS Strategy the following key areas were outlined:

- The journey undertaken by the STS since the previous Strategy had been reviewed, focussed around building a sustainable shared service, improving stability and delivering continuous improvement supported by specific case studies from each member authority.

- The core elements of IT and Digital technology functions managed across the STS for all partner authorities along with breakdown of services managed within each Council.

- The core values identified by the STS in seeking to serve the partners they supported focussed around collaboration, improve, care, serve and openness.

- The vision for the STS to deliver an outstanding and leading public sector technology service for the benefit of its organisations supported by a mission "to provide a secure, reliable and cost-conscious service which always strives for improvement, enabling partners digital ambitions".

- The outline of key challenges faced by the STS in seeking to deliver the Strategy including financial pressures, change in working patterns, climate emergency and need for services to become more sustainable, pace of technological change (including AI, cyber security) and increased reliance on data, integration and focus on customer experience.

- The ongoing focus within the Strategy in maintaining a collaborative partnership approach between the STS and partner authorities.

- The key areas of focus within the Strategy relating to financial value, cyber security, service and technology, wellbeing and environment along with the

challenge, objectives and commitments identified across each area in relation to ongoing delivery of the STS and future service development in support of the overall vision and mission identified.

The chair thanked Fabio Negro for the outline provided in relation to the Strategy with comments then invited from members and the following issues raised:

- In noting that the pace of technological change had been identified as a key challenge in seeking to develop the new Strategy, further clarification was sought on the way this had been reflected within the Strategy to provide the necessary flexibility, particularly recognising the nature and pace of change in digital technology. In response, Fabio Negro advised this had been recognised as an ongoing challenge within the service with the Technology Road Map having been developed in response and subject to annual review and refresh to ensure significant changes in the landscape could be reflected and planned for moving forward.

  In support of the approach identified as a means of being able to plan, adapt and evolve the Road Map, members advised they were keen to ensure that the Strategy remained as flexible as possible with any update or changes agreed as a result subject to review and monitoring through the Joint Committee. In responding, Fabio Negro advised that the need to build in regular progress checkpoints and updates on delivery and any changes in the Strategy had already been recognised by the STS moving forward, in order to reflect progress on development of the future Technology Investment Plan and refresh of the Technology Road Map.

- In recognising and welcoming the reference to delivery of social value included within the Strategy, members highlighted a need to ensure this approach was maximised in relation to not only the procurement process but also in terms of broader benefits such as engagement with local businesses, the delivery of employment and training opportunities and also digital inclusion.

  In seeking to further develop this as an overall approach, members also requested that as part of a future update for the Joint Committee an outline be provided on the broader social value deliverables across each partner authority through the services being delivered by the STS and how these also linked to the key strategic corporate priorities identified by each Council.

- The need identified to ensure the impact and lessons learnt from incidents relating to service delivery were also reflected as part of the approach outlined within the Strategy relating to Service and Technology. As an example, reference was made to a recent incident involving a Firewall update which had impacted on a public committee meeting without advance notice being provided to the partner authority. In recognising the political and reputational impact, members therefore sought reassurance that the Strategy would include the ability to reflect on lessons learnt from these type of incidents including the need to develop appropriate communication plans, which members were advised had already been recognised by the STS.

As no further comments were raised in relation to the STS Strategy, the Chair then moved on to invite Ciaron Weldon (as Chief Information Security Officer for the STS) to present the STS Cyber Security Strategy 2024-26 for which approval was also being sought from the Joint Committee.

In presenting the Cyber Security Strategy the following key areas were outlined:

- The key challenges identified in relation to addressing cyber security across the STS partner authorities with a key focus based on the controls in place to protect and react against cyber threats and protect not only each Council but also their customers and residents.

- The purpose and scope of the Strategy, recognising the scale of digital transformation activity and emerging technology and need to provide and embed robust information and cyber security measures.

- The key building blocks involved in developing the Strategy at basic, foundation and organisational levels

- The review of assets and vulnerabilities undertaken in seeking to develop the Strategy, alongside the outline of threats identified both internally and externally and strategic approach developed in response in seeking to mitigate against the threats and risks identified. This had included enhancements to the STS Cyber Security resource and initiation of a 3rd party security operations centre service to support the ability to detect and respond to cyber security related incidents in real time along with the establishment of a cyber security vulnerabilities team all aligned with the National Cyber Security Strategy.

- The key areas of activity identified within the Strategy and Implementation Plan which had been designed to recognise the different levels of maturity and capacity in relation to the approach within individual partner authorities, focussed around:
  - ➢ DETECT – which had involved the STS developing the ability to detect, on a pre emptive basis, potential cyber events based around an approach involving asset management, baseline establishment, threat intelligence and continuous monitoring,
  - ➢ DEFEND – which had involved STS developing the means to defend against evolving cyber threats, respond effectively to incidents, and ensure networks, data and systems were protected and resilient.
  - ➢ DETER – which had involved STS detecting, understanding, investigating, and disrupting hostile activities against the service.
  - ➢ DEVELOP – which had involved STS developing a coordinated and tailored approach to risks and threats encountered and mitigating against potential vulnerabilities.
  - ➢ REACT – which had involved STS in developing sufficient controls to respond to any attacks including the organisational channels and processes required to make efficient decisions further protect data and limit any scope of attack.

- The supporting activity to provide ongoing assurance on the effectiveness and robustness of the STS arrangements to delivery IT security along with key roles and responsibilities outlined within the Strategy aligned with the cyber assurance framework.

The chair thanked Ciaran Weldon for the outline provided in presenting the Strategy with comments then invited from members and the following issues raised:

- Members welcomed and supported the approach and focus outlined within the Strategy in seeking to address and mitigate against the key cyber security risks identified balanced against the business needs of each partner authority. Further details were sought on the process involved in seeking to monitor and assess trends and threats being identified, which members were assured included continuous review and engagement with key stakeholders including the Council's 3rd party security operations centre service and National Cyber Security Agency.

- In response to details regarding the management and mitigation of potential cyber security risks associated with the use of systems by 3rd party suppliers, members were advised and noted the approach adopted in seeking to ensure suppliers were aligned with the necessary STS and individual authorities cyber security requirements.

- Further details were sought on the Emergency Planning Cyber exercises which it was noted had been held across all three partner authorities and members were advised had been focussed across a range of command level participants and services and the arrangements to enhance business continuity and contingency planning process. Workshops focussed on lessons learnt to facilitate efficient resource and outcome sharing among STS and partner organisations had also been held, with members keen to ensure these exercises in future also involved the opportunity for councillor involvement.

- In noting the number of security related risks which had been identified within the top risks listed for the STS in section 6.2 of the STS Performance Update report, members felt it would be useful to include a more strategic overview (including relevant mitigations) as part of future updates on trends in relation to the current risk level scores.

- As a a final issue, members advised (as with the STS Strategy) they would also be keen to ensure any update or changes agreed in relation to delivery of the Strategy were subject to review and monitoring through the Joint Committee with progress updates also provided at relevant stages in delivery of the Strategy.

As no further issues were raised, the Joint Committee completed their consideration of the update report. The Chair thanked officers for the updates provided and it was **RESOLVED**:

(1) To note the update provided and actions being taken in relation to the ongoing performance and delivery of the Shared Technology Service, as detailed

within the report along with the briefing provided on the response to the CrowdStrike incident (as detailed within Appendix 1 to the report) and review on the Laptop Refresh Project procurement process (as detailed within Appendix 2 of the report).

(2)   To approve adoption of the STS Strategy 2024-26 as detailed within Appendix 3 of the report.

(3)   To approve adoption of the STS Cyber Security Strategy 2024-26 as detailed within Appendix 3 of the report.

(4)   To agree as further actions related to (1) – (3) above:

(a)   The provision of details within future update reports on STS performance relating to metrics associated with STS call wait times and also a more strategic overview in relation to trends association with key risks identified within the STS Risk Register.

(b)   that the Joint Committee continue to be provided with monitoring updates on delivery of the both the STS and STS Cyber Security Strategies 2024-26 including any changes agreed as a result of their ongoing review and implementation.

(c)   that a future update be provided for the Joint Committee on the broader social value deliverables being delivered across each partner authority arising through the services being delivered by the STS and how these were also linked to the key strategic corporate priorities identified by each Council.

7.   **Date of Next Meeting**

Members noted the following dates scheduled for future meetings of the Joint Committee during 2024-25 Municipal Year:

- Tuesday 18 March 2025 at 6pm – to be held online chaired by the London Borough of Brent.

8.   **Any Other Urgent Business**

None identified.

9.   **Exclusion of Press and Public**

At this stage in proceedings the Chair advised that she intended to move into closed session for the remainder of the meeting in order to consider a separate report for the Joint Committee providing updates on the Cyber Security status, threats, and mitigations in relation to the Shared Technology Services (STS).

Given the commercially sensitive nature of the details contained within the update, the Joint Committee were advised that the report would need to be considered in closed session which would require the Joint Committee to pass a formal resolution excluding the press and public for consideration of the item.

It was therefore **AGREED** that that under Section 100A (4) of the Government Act 1972 the press and public be excluded from the remainder of the meeting for consideration of the following item on the grounds that it would involve the disclosure of exempt information as defined in paragraph 3 (information relating to the financial or business affairs of any particular person, including the authority holding that information) of Part 1 of Schedule 12A of the Act (as amended).

10. **Shared Technology Service Cyber Security Update Report**

Fabio Negro (Managing Director - Shared Technology Services) then introduced the update report in relation to Cyber Security status, threats, and mitigations for the Shared Technology Service (STS). In considering the report members noted:

- The outline of events impacting on STS along with an update on current threats and mitigating actions in relation to the following key areas of activity as detailed within section 3-7 of the report – Defend, Deter, Develop and React.

- The outline of future plans being developed in relation to the STS Cyber Security Strategy, as detailed within section 8 of the report, which had included a project focussed on future laptop design (now in delivery phase) as well as work to develop the plans for implementation of Microsoft's biometric authentication method for logging into devices and replace current web-filtering solutions.

The Chair thanked Fabio Negro for his update with additional clarification provided for members in relation to the following issues raised:

- The background and resolution of recent cyber security events impacting on the STS across each borough, including the costs and resources involved in dealing with incidents.

- The approach being developed towards the use of biometrics as a potential security feature across individual partner authorities, on which a further update was requested at a future meeting of the Joint Committee including proposals for an appropriate communication plans.

- The approach being developed to monitor the evolving nature of risks and threats and ensure the necessary mitigations and business continuity and resilience arrangements were place across each partner authority, as part of their incident response planning process.

As no further matters were raised, the Joint Committee completed their consideration of the update report. The Chair thanked Fabio Negro and Ciaran Weldon for the details provided and it was **RESOLVED** to:

(1) note the update and actions being taken as detailed in the report.

(2) To request (in view of the issues highlighted during the meeting) a future update was provided for the Joint Committee on the approach towards the use of biometrics as a potential security feature on devices to be included within

the laptop refresh programme including a focus on the communication plans being developed for users.

The meeting closed at 7.07 pm

COUNCILLOR STEPHANIE CRYAN
Chair