MINUTES OF THE JOINT COMMITTEE OF THE LONDON BOROUGHS OF BRENT, LEWISHAM AND SOUTHWARK
Held as an online meeting via MS Teams on Tuesday 17 March 2026 at 6pm

PRESENT (as online participants): Councillor Amanda De Ryk (Chair - London Borough of Lewisham), Councillor Stephanie Cryan and Councillor Barrie Hargrove (London Borough of Southwark) and Councillor Jake Rubin and Councillor Mili Patel (London Borough of Brent)

1. **Appointment of Chair**

It was **RESOLVED** that in accordance with Section 10 of the Joint Committee's Terms of Reference, Councillor Amanda De Ryk (London Borough of Lewisham) be appointed as Chair for the duration of the meeting.

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

No apologies were received.

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 25 November 2025 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**

Prior to presenting the update report, Fabio Negro (Managing Director Shared Technology Services) took the opportunity to introduce Stuart O'Shea to the Joint Committee as the Shared Technology Service's (STS) newly appointed Head of Operations.

Fabio Negro informed the Committee of the two recent deaths in service; Tim Green, Head of Strategy and Technology and Frank Lee, Cyber Security Analyst whose deaths have left the service saddened, as they were key members of the team and will be sadly missed. The Chair sent her condolences on behalf of the Joint Service to the team and the families involved. Fabio Negro said that he will share the news across the service.

Fabio Negro then 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 was advised of the following:

- In this reporting period (November 2025 to February 2026), SLA performance for priority 3 (P3) operational incident issues had improved and priority 4 (P4) operational request calls SLA had been maintained within the SLAs in the main.

- In this reporting period (November 2025 to February 2026), SLA performance for P3 operational incident issues and P4 average SLA operational request calls SLA had improved when compared with the previous reporting period. This resulted in a reduction in open calls and showed good progress in overall operational performance with the lowest number of open calls recorded in December 2025.

- During the same reporting period, there were 10 P1 incidents related to STS infrastructure.

- There were 13,003 P3 logged calls during the reporting period, which was a slight increase on Jul-Oct 2025 (1%).

- Software applications (38%), Hardware tickets (22%), Email (9%) and Connectivity (8%) represented the largest share of raised ticket types.

- STS was currently in the 4th year of the 5-year investment plan with the majority of the infrastructure transformation having been delivered. Over the next calendar year, all laptops will be upgraded to Windows 11 or replaced. This replacement was underway in all three Councils, with Brent now largely finished. New laptops were being rolled out in Lewisham with good progress being made and the majority of staff at Southwark now had new laptops.

- Microsoft Defender: a set of security tools designed to protect against cyber threats and included in Microsoft M365 licensing. Using these tools will produce significant costs saving to partners. Microsoft Defender for Cloud project was initiated in November 2025 to replace the incumbent server security software, CrowdStrike. It had since been rolled out across the server infrastructure for all partners and the LGA, successfully completing in February 2026. The project was winding down and was scheduled to close March 2026.

- Core Network Firewall Replacement: this project successfully completed in February 2026. This project replaced the legacy core firewall platform, which had reached end-of-life, with a modern next-generation solution to strengthen the network security and resilience for all STS partners. The new platform provided enhanced protection against emerging cyber threats, improved visibility of network activity and greater capacity to support cloud services and hybrid working. The upgrade removed the risk associated with unsupported

infrastructure and positions the organisation to respond more effectively to evolving security threats, while supporting future digital growth.

- Azure Arc Roll-out: project completed successfully in December 2025. This moved the management of the services from a on-premises server management platform to the cloud, regardless of whether the server was on-premises or hosted in the cloud. While core systems remained appropriately hosted within data centres, this initiative enabled them to be managed using modern cloud-native capabilities. This included centralised policy enforcement, enhanced security monitoring and improved compliance reporting, delivered through the Azure control plane. Southwark had migrated to Azure a number of years ago.

- The project represented a deliberate step towards a cloud-first operating model, focusing on adopting cloud-native management, automation and governance services rather than simply relocating virtual machines. It strengthened security oversight, improved consistency across partner environments and provided a scalable foundation for future digital transformation.

- The aim of migrating email security to Microsoft Defender was to replace Proofpoint for Office Microsoft 365 and Fortra. Professional services provided by a third party were used to expedite the process to avoid renewal of the costly Proofpoint contract. To date, the migration to Microsoft Defender for email security had been successfully completed by STS across all partners and now protected approx. 11,000 users.

- A major cost efficiency had been secured through the strategic replacement of Proofpoint email filtering services, previously costing £306k, with a new solution from Fortra delivered at £38k. This transition had produced a total saving of £268k across the Shared Service, while maintaining (and in areas improving) the required email hygiene and threat protection standards. The move to Fortra also positioned the partnership for smoother integration with Microsoft's Defender ecosystem should future alignment be pursued, creating optionality while already delivering substantial financial benefit.

- As a final update, Members were advised that Southwark had now provided notice to exit the Shared Service and will leave in March 2028. Plans were being drawn up to incorporate new teams and principles going forward.

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

- Councillor M. Patel noted the positives around the lowest number of open calls being recorded in December 2025 and noted that numbers rose again in January 2026 and asked whether this was due to the Christmas period. Stuart O'Shea explained that historically a rise of 14% had been seen following the Christmas holidays. Fabio Negro added that following analysis, it was identified that STS received approx. 50 additional calls per week due to the laptop rollout projects.

- Councillor Hargrove asked for the graphs and tables on the report to be titled and queried why there were so many P2 incidents at Southwark. Fabio Negro explained that this was due to the laptop roll out as well as other projects that STS were working on. Councillor Hargrove asked if a P2 incident meant a loss of service for a period of time. Fabio Negro said that a P2 was a serious issue that was defined as an incident that resulted in either unavailability or degradation of a service which, whilst material, did not meet the threshold for a P1. P1 incidents affected critical Council functions.

- Further details were sought on SLAs for closing open tickets. Fabio Negro stated that there were SLAs for the number of tickets raised for P1 and P2 incidents. There was an aim to have less than 3 P1 incidents and less than 15 P2 incidents per month. There was an aim to close P3 incidents within 8 hours of the ticket being opened. The team met 90% of the SLAs for P3 incidents and 80% for P4 incidents.

- Members asked for assurance of tickets being closed at the earliest opportunity. Fabio Negro said that there had been an issue with reporting, which was remedied by the team presenting pre-delivery reports. P3 incidents had finally reached normal levels in the past 5 years. Tim Green, who had passed away was the head of reporting and any data needed will be ready for the next meeting.

- Whilst noting that valuable lessons had been learnt from the P1 incidents, Members asked how STS planned to protect savings with the loss of a key partner – Southwark. Fabio Negro noted that STS did indeed make savings through joint procurement and this may still continue post exit. Additionally, there will still be benefits post exit.

As no further issues were raised, the Joint Committee completed their consideration of the update report. The Chair thanked Fabio Negro for the updates provided and it was **RESOLVED** to note the progress being made across the various areas in the detail of the report including the Inter-Authority Agreement and Southwark Council's notice to exit the partnership, as outlined in the report.

7. **Date of Next Meetings**

Members NOTED the provisional list of dates for the Joint Committee during the 2026 – 27 Municipal Year as follows:

- Tuesday 7 July 2026 - Brent to host online – 6pm
- Tuesday 17 November 2026 - Southwark to host online – 6pm
- Tuesday 16 March 2027 - Lewisham to host online – 6pm

These dates were currently being finalised and will then be subject to confirmation by each respective partner borough.

8. **Any Other Urgent Business**

None identified.

9. **Exclusion of Press and Public**

At this stage in proceedings the Chair advised that he 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).

The online livestream was ended at this point in the meeting.

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).

Members were advised that there had been no serious breaches or significant changes since the last meeting except the risk relating to the conflict in the Middle East.

In considering the report Members noted the update provided in relation to the server Extended Defence and Response service transition from CrowdStrike to Microsoft Defender for Cloud, with NCC assuming responsibility for monitoring alerts via the SOC, this followed NCSC best practice. This transition provided comprehensive visibility into incidents across the entire estate, resulting in improved response times and more efficient escalation processes. Full migration was completed in February 2026.

Following the findings from the PSN IT Health Check, STS were collaborating with partners to strengthen the authentication framework. This included aligning password policies with the FIDO standard and implementing multi-factor authentication (MFA) using phishing-resistant technologies. STS had also initiated strategic engagement with Microsoft to enhance user identity security and service monitoring capabilities

Members were also provided with an update on the recent cyber security attack which had affected a shared IT infrastructure environment across three London Councils, who were not members of the STS. In noting the initial background provided, members noted the measures in place across STS to mitigate against a similar type of incident and assistance which had been offered to the boroughs affected as they sought to respond and recover. The need to ensure continued

vigilance in terms of the defence against evolving cyber threats was recognised by the Joint Committee in order to ensure STS was able to respond effectively to incidents, and ensure networks, data and systems remained protected and resilient.

STS recently delivered a series of Cyber training sessions,. The programme had been designed to strengthen the cyber resilience of STS by providing practical, up to date, NCSC assured and CPD certified guidance on recognising and responding to cyber threats. Across sessions held, staff received in person training covering modern cyber-crime techniques, real world case studies, incident response principles and actionable steps for protecting personal and organisational data. Feedback from attendees was extremely positive, highlighting the clarity of the sessions, the relevance of the examples and the engaging delivery style.

The Chair thanked Fabio Negro for the update and said that it was interesting to note the learning from the tri-borough incident and added that she was in support of the training being rolled out with further clarification also provided (in response to member queries) relating to reference to the term ‘social engineering’ and impersonation.

As no further matters were raised, the Joint Committee completed their consideration of the update report. The Chair thanked Fabio Negro for the details provided and it was **RESOLVED** to note the update and actions being taken as detailed in the report.

The meeting closed at 7:09pm.

COUNCILLOR AMANDA DE RYK
Chair