NEWARK & SHERWOOD
DISTRICT COUNCIL

Report to: Audit & Accounts Committee Meeting 10 December 2025

Director Lead: Sanjiv Kohli, Deputy Chief Executive/Director of Resources (S151 Officer)

Lead Officer: Dave Richardson, Business Manager – ICT & Digital Services Ext 5405

Report Summary	
Report Title	Update on the LGA Newark and Sherwood District Council Cyber 360 Report
Purpose of Report	To present the updated results of LGA Newark and Sherwood District Council Cyber 360 Report
Recommendations	Members review, comment upon and note the update on the LGA Newark and Sherwood District Council Cyber 360 Report
Reasons for Recommendation	To provide Members with details and assurance from the LGA Newark and Sherwood District Council Cyber 360 Report

1.0 Background

1.1 The Local Government Association piloted Cyber 360 (C360s) peer reviews with several Local Authorities to ensure Cyber and information Security governance and culture is being understood and adequately resourced. The Cyber 360 Action Plan is not in the public area of the open report for security reasons and are held in the exempt version.

1.2 At the September 2023 Audit & Governance Committee the ICT & Digital Services Business Manager provided an update on the Cyber360 action plan and assurance that we are addressing any areas of cyber risk.

1.3 A Cyber360 action plan has been commissioned off the back of the report and regularly updated by the Corporate Information Governance Group (CIGG). Therefore, the updates to this committee will be provided by exception, on request or at least on an annual basis.

2.0 Proposal/Options Considered

2.1 The CIGG will continue the review of the Cyber360 action plan and provide updates. As of December 2025, 92% of the action plan is complete, with only 2 out of 24 tasks remaining.

2.2 It is important to note that further controls and measures have been implemented to enhance the Council's cyber resilience in alignment and exceeding the cyber security strategy 2022-2026.

2.3 Cyberattacks are constantly evolving and becoming more sophisticated. As councils undergo reorganisation and mergers, communicated in the public domain, we are more likely to undergo additional attacks and therefore it should be noted that the overall strength of our collective cybersecurity is determined by each individual partner. Since systems and resources are shared, a vulnerability in one council can impact all. It is essential to maintain robust cyber resilience across all partner councils to safeguard shared services and data. Consequently, we should advocate for adopting the highest standards and best practices.

2.4 Therefore, this report is intended to provide assurance to our partners and communities that we approach our responsibilities with the utmost seriousness now and into the future unitary Council.

2.5 Lastly, it should be noted that that on 24 November 2025, a major cyber incident affected shared IT systems across three London councils, disrupting critical services and phone lines. Authorities confirmed some historical data was accessed, but operational systems remained available. Although there’s no clear evidence of personal data compromise, residents were alerted, and the Information Commissioner’s Office was notified. Councils focused on restoring services, protecting vulnerable individuals, and working with cyber specialists to eliminate threats. The event highlights the risks in shared-service models and the need for strong cyber resilience in local government especially with LGR gaining momentum for Nottinghamshire Councils.

3.0 Implications

None.

Background Papers and Published Documents

Except for previously published documents, which will be available elsewhere, the documents listed here will be available for inspection in accordance with Section 100D of the Local Government Act 1972. Any documents that contain confidential information or personal information about individuals should not be included in this list.