Report of the Data Protection Officer

AUDIT AND GOVERNANCE COMMITTEE – 31st May 2023

DATA PROTECTION OFFICER ASSURANCE REPORT

1. Purpose of the Report

1.1 This report highlights the key areas of work of the Council's Data Protection Officer (DPO) to provide the Committee with information and assurances regarding the Council's compliance with the Data Protection Act 2018 and UK GDPR.

2. Recommendation

2.1 It is recommended that the Committee consider the report and the information and assurances within it and receive a further update in 6 months' time to contribute to wider and continuous assurances as part of the Annual Governance Review process.

3. Background

3.1 The Council is required to appoint a DPO under the General Data Protection Regulations and Data Protection Act 2018. The key aspect of this role is to provide the Council with independent assurance regarding compliance with data protection law.

4. Assurance Update

4.1 The DPO has regular meetings with officers from the Information Governance and Security Team and the Senior Information Risk Officer (SIRO) and reports to the Information Governance Board. The DPO also undertakes or commissions specific assurance reviews to support that independent assurance, when required.

4.2 Overall, recent activity and general oversight, continues to provide a generally positive picture regarding compliance with UK GDPR. To support that, the Information Governance Board provides a clear focus on compliance and awareness. Strategic issues are escalated to the Senior Management Team as required thus ensuring data protection, security and general information governance matters are considered at the highest level.

4.3 The Information Governance and Security Team have continued to provide regular reminders to all staff regarding various aspects of information governance, as well as mandatory training through the POD on-line training

system. Such mandatory training has covered information governance generally, incident management, protecting personal data, subject access requests and a general UK GDPR reminder. The take-up of mandatory training is relatively good with around 85% of networked employees completing the training. The figure is around 40% for non-networked employees where they receive verbal briefings from team managers. This is an area of particular focus of the Information Governance Board.

4.4 Compliance with the statutory timescales for responding to FOI and SAR requests remains very high at over 98% which reflects the work undertaken to support staff receiving such requests and significant improvements in the system that manages requests and responses making it easier and more efficient for services to meet the timescales.

4.5 During 2023, there have been three phishing campaigns which have also highlighted improved awareness amongst staff to spot any irregular emails and report them to IT. This threat is further mitigated by the comprehensive technical framework in place to prevent malicious emails and general cyber-attacks entering the Council's network and systems. However, it is acknowledged that whilst employee awareness is good and good technical measures are in place, attacks from phishing and whaling remain a high risk to the Council and rely on staff being constantly alert to the risk. Incidents at other councils highlight the significant risk posed by phishing and whaling attacks.

4.6 Significant work continues to be undertaken around cyber and IT security generally. Password cracking exercises are periodically undertaken to ensure high levels of awareness and firm security posture. It remains a priority of the Information Governance and Security Team to constantly reduce the number of data incidents and help improve the timeliness of management actions to minimise the risk of incidents recurring. There has been a steady reduction in incidents over the last 3 years and this continued during 2022/23. An analysis of data incidents is presented to the Information Governance Board for monitoring.

4.7 The Information Governance and Security Team along with the Emergency Resilience Team have run a number of simulated cyber-attack exercises with leaders across the Council to raise awareness and highlight any areas where improvements are needed to ensure we are able to respond should an attack be successful and render IT systems unavailable. These exercises were very useful with follow-up work being planned to ensure that resilience. The threat from a cyber-attack is a key strategic risk discussed at Senior Management Team and Cabinet level given the impact attacks have had on a number of other councils.

4.8 The DPO is regularly contacted to provide advice and guidance on data protection concerns and particularly where the Information Commissioner's Office is involved in a matter.

4.9 The DPO undertakes or commissions independent reviews of various aspects of information governance. Those undertaken in 2022/23 have been:

Area Covered	**Key Issues**
CCTV review (on-going)	Oversight of work to ensure compliance with best practice in the use of CCTV across the Council.
Incident management (Feb 2023)	Reasonable assurance. Key issue was ensuring there was consistency in reviewing incidents and providing evidence of closure of the incident and follow up of lessons learned.
Cyber security (March 2023)	Limited assurance. At the time of the review a number of policies required review and the PSN accreditation was due. This remains outstanding but is scheduled to be achieved by the end of June. Policies have now been reviewed. The Cyber team and DPO will attend Scrutiny Committee on 6th June 2023 to present the developments made over the last 12 months to elected members.
DPIA review and compliance (Dec 2022)	Limited assurance. Key issue was the need to ensure DPIAs were reviewed and that responsibility was re-assigned where staff had changed roles or left the Council. The DPIA process is undergoing a full review which will improve management assurances, providing a streamline and dynamic eform.
Information sharing agreements (on-going)	Oversight of work to create and maintain a corporate process to manage data/information sharing agreements.
Data retention / records management (Feb 2023)	Limited assurance. Key issues raised were the capacity of the Records Management Team to adequately support services in their responsibilities, and issues around legacy systems holding data beyond normal retention periods. SMT have requested a Records Management Strategy to be developed, due for release June 2023.

4.10 In all cases management actions have been implemented as agreed or are on schedule for completion by the agreed dates.

4.11 A key issue raised and discussed at the Information Governance Board is to review the role of information asset owners across the Council. This role is key to embed good awareness and compliance with various aspects of information

governance within services. It is important to stress that corporate arrangements for information governance management are good. There does however need a renewed focus to ensure services are fully aware of their responsibilities to maintain those good levels of compliance.

4.12 The DPO and Internal Audit will continue to monitor management's response to the issues raised and conduct further independent reviews and audits on a continuous rolling basis. These will be reported to the Information Governance Board and the Audit and Governance Committee.

4.13 As a key source of assurance for the Committee and to properly discharge the responsibilities of the DPO, the role requires independence from management, unfettered access to senior management and access to the necessary resources. These key requirements are in place.

4.14 As stated, overall, the Committee can be assured that whilst there will inevitably be data and information incidents there is a robust and comprehensive suite of policies and guidance in place supported by a strong and committed Information Governance and Security Team. The joint working and liaison between the DPO, Information Governance, Cyber Security, the SIRO, and Legal Services provides a robust basis to guide the Council to ensuring that data protection responsibilities are understood and complied with as effectively as is reasonably possible.

4.15 A section within the Annual Governance Statement is also included to provide the assurances from the DPO.

Contact Officer: Data Protection Officer
Email: DPO@barnsley.gov.uk
Date: 17th May 2023