Report of the Data Protection Officer

AUDIT AND GOVERNANCE COMMITTEE – 15th November 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 continues to have 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 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 Council staff regarding various aspects of information governance and cyber threats as well as training through the POD on-line

training system. Such training covers information governance generally, incident management, agile working, protecting personal data, subject access requests and a general UK GDPR reminder. The take-up of training is good amongst networked employees.

Course Title	% Completed
Information Governance	96%
Incident Management	86%
Agile Working	85%
Protecting Personal Data	85%
Subject Access Requests	81%
UK GDPR	91%

The figure is around 30% on average for non-networked employees. Improving the take-up of this training is being reviewed in terms of making access to the courses easy, but also ensuring they are relevant to the type of employee. This is an area of particular focus of the Information Governance Board.

4.4 Compliance with the statutory timescales for responding to Freedom of Information requests (FOIs), subject access requests (SARs) and Environmental Impact Assessment requests (EIAs) remains very high at 99% for FOIs, 86% for SARs and 100% for EIAs. This 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. A number of very complex SARs are currently in progress that have gone beyond the statutory timescales, but officers are working closely with the requestors to meet their requests. Where problems do occur in meeting the timescales, there is a review process in place to identify and learning to minimise the risk of delays occurring in the future.

4.5 During 2023, there have been a number of simulated phishing campaigns which aim to reinforce awareness amongst staff to spot any irregular emails and report them to IT. Where an employee fails the test, they are immediately directed to a training video, receive feedback on the email, pointing out the errors or in an infographic.

4.6 The threat posed by phishing attacks 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.

4.7 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 a firm security posture. Further password strengthening is to be enforced in January. 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. An analysis of data incidents is presented to the Information Governance Board for monitoring.

4.8 The Information Governance and Security Team along with the Emergency Resilience Team ran 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.

4.9 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. This is a positive in staff being aware of the DPO and their role.

4.10 The DPO undertakes or commissions independent reviews of various aspects of information governance. There are a number of specific pieces of assurance work planned for 2023/24. These are:

- Data Management
- Information system archiving arrangements
- Cyber Strategy
- Cyber Emergency Resilience Arrangements

4.11 The implementation of the agreed management actions arising from the previous pieces of assurance work are being monitored by Internal Audit as part of their processes.

4.12 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, but there does however need a renewed focus to ensure services are fully aware of their responsibilities to maintain those good levels of compliance.

4.13 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.

4.14 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.

4.15 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.

4.16 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: 1st November 2023