Item 11

Report of the Data Protection Officer

AUDIT AND GOVERNANCE COMMITTEE - 16TH NOVEMBER 2022

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 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 Team and the Senior Information Risk Officer (SIRO) and reports to the Information Governance Board. The DPO also undertakes specific assurance reviews to support that independent assurance.

4.2 Overall, recent activity and general oversight, continues to provide a 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 and general information governance matters are considered at the highest level.

4.3 The Information Governance 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 incident management, protecting personal data, subject access requests and a general UK GDPR reminder. The take-up of mandatory training 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 is very high which reflects the work undertaken to support staff receiving such requests and the diligence of the Customer Feedback and Improvement and Information Governance Teams. Further work is continuing to improve the supporting system that will enable officers to respond to FOI and SAR requests more efficiently and effectively.

4.5 Phishing campaigns 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 associated with phishing and whaling attempts.

4.6 Significant work continues to be undertaken around cyber and IT security generally. A recent password testing exercise was undertaken to ensure high levels of awareness and security. It remains a priority of the Information Governance 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. An analysis of data incidents is presented to the IG Board for monitoring.

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

4.8 The DPO undertakes or commissions independent reviews of various aspects of information governance. Those planned for 2022/23 are

DPO Assurance:

- CCTV review
- Incident management
- Cybersecurity
- DPIA review and compliance
- Information sharing agreements

Internal Audit:

- Data retention / records management
- Customer Feedback and Improvement Team follow-up

4.9 Additional review work will obtain assurances regarding:

- Redaction capacity development and effectiveness
- Review of SAR procedures and implementation of actions
- Data Sharing Agreement progress
- Detailed review of the IG risk register
- Mandatory training plans and take-up
- General use of IG related management information / dashboards

4.10 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.

4.11 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.

4.12 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 Team. The joint working and liaison between the DPO, Information Governance, the SIRO, Customer Feedback and Improvement Team 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.

4.13 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:	7th November 2022