

Report of the Data Protection Officer

AUDIT AND GOVERNANCE COMMITTEE – 17TH November 2021

DATA PROTECTION OFFICER UPDATE REPORT

1. Purpose of the report

- 1.1 This report highlights the 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 the data protection law.

4. DPO Activities

- 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 Recent assurance reviews and general oversight continue to present a positive picture overall. The change in focus of the Information Governance Board has provided a clearer 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 A major review of how the council responds to information requests under the Freedom of Information and Data Protection Acts has been effective in significantly improving compliance and meeting the necessary timescales for response. A number of information and data requests are however very time consuming and demand significant resources from services to collate the information/data requested and in certain cases apply complex and detailed redactions. This issue is being considered by the Information Governance Board

to explore how best these particularly demanding requests continue to be met in an appropriate timescale and to the necessary quality with minimum impact on core service delivery.

- 4.4 Significant work is also being undertaken around cyber and IT security, with regular phishing and password testing exercises to constantly ensure high levels of awareness and security. It was recognised again as part of the annual governance review process however that there remains scope to try and further reduce the number of data incidents and improve the timeliness of management actions to minimise the risk of incidents recurring. Actions in that regard are in place and are monitored by the Information Governance Board and the Committee.
- 4.5 Data incidents do of course occur. Information regarding these is available for managers via a dashboard therefore enabling more effective awareness and management action.
- 4.6 A review of cyber security looking at progress against the IT Security Strategy has been completed for which a Reasonable (positive) Assurance opinion was given.
- 4.7 The further areas of review and audit to be undertaken over the next 6 months are:

DPO Assurance:

- CCTV review
- Incident management
- Contract provisions
- Law Enforcement
- DPIA review and compliance
- Information sharing agreements

Internal Audit:

- Data retention / records management
 - CFIT follow-up
- 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 As an example of DPO work, a significant amount of time has been taken up over the last 12 months supporting management in a particularly complex and sensitive matter. This matter has highlighted a number of areas for management to consider and review involving data quality, information systems and the management of complex requests.

- 4.9 Another example involved another complex data breach allegation and whilst no data breach is considered to have been made, it has highlighted the need for certain information sharing agreements (ISAs) to be reviewed. This is being picked up in the wider corporate review of ISAs. Being involved in specific significant matters provides opportunities for wider corporate learning and the development of better training, advice and guidance.
- 4.10 A rolling programme of assurance reviews is maintained, akin to an audit plan. This is reviewed annually and shared with the Information Governance Board.
- 4.11 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.
- 4.12 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.
- 4.13 As stated, overall, the Committee can be assured that whilst there will inevitably be data 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 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.

Contact Officer: Data Protection Officer
Email: DPO@barnsley.gov.uk
Date: 8th November 2021