Sunderland City Council

Item No. 8

AUDIT AND GOVERNANCE COMMITTEE **21 July 2023**

DATA PROTECTION – ANNUAL REPORT 2022/23

Report of the Data Protection Officer

1. Purpose of Report

1.1 The purpose of this report is to provide the Committee with information about the work and findings of the Council's Data Protection Office during the past year.

1.2 The Committee is asked to consider the:

- Data Protection arrangements outlined in this report.
- Performance against Data Protection standards in the 2022/23 year.

2. Background

2.1 The Council has designated a Data Protection Officer (DPO) as required by Data Protection law, to advise on its data protection compliance responsibilities and act as its point of contact with the Information Commissioner's Office (ICO). The Council has historically received support with Data Protection (DP) compliance from the Council's Data Protection Office, a Strategic Information Governance Group made up of senior officers and chaired by the Director of Finance in the role of Senior Information Risk Officer (SIRO). The Data Protection Office also provides a DPO service under service level agreements to connected organisations, including the Council's wholly owned companies, the NECA and those schools and academies which subscribe to the service.

2.2 A revised Information Management Policy and Strategy (IMPS) was approved by Chief Officer Group in October 2021. The IMPS is designed to reflect changes to working arrangements and priorities imposed by the Council's response to Covid, the migration to the Office 365 Microsoft Teams environment and the move to City Hall.

2.3 A key feature of the IMPS was the refresh and reiteration of the role of Information Asset Owners (IAOs) as a critical function for considering risks associated with the information held within their service areas, monitoring compliance with the legislation, and disseminating and implementing arrangements to meet compliance requirements. The IAO role sits with Assistant Directors within the Council.

2.4 The Data Protection Office continues to provide advice and guidance to support IAOs and service areas with DP compliance. During 2022/23, the

DPO team continued to work with the Transformation Project Team and Corporate Support Service, which has led to the development of comprehensive new Information, Advice and Guidance materials and training packages to support IAOs and staff, allowing them to 'self-serve'.

2.5 As a data controller, the Council remains obliged to pay an annual fee and is registered as a fee payer with the ICO, as are Together for Children, Sunderland Care and Support, Siglion and the IAMP. Schools and Academies are also required to pay the annual fee as individual concerns. Elected Members are no longer required to pay a fee and so do not maintain individual registrations with the ICO. Members nevertheless remain data controllers of the information they process in carrying out their ward work, with responsibility for data protection compliance when managing the associated information.

2.6 The Council also acts as a data processor in relation to some of the information it processes (the People Management and Payroll services offered to customer organisations as two examples), and as data controller in common or joint data controller with its companies and other partner organisations. Other organisations and contractors act as data processors on behalf of the Council and its connected organisations; standard contract clauses, data processing schedules and cyber-security standards have been incorporated to reflect current DP requirements of processors.

2.7 The Council and its companies continue to work in partnership with other organisations, including other councils, health partners, the Police and voluntary and community services under formal information sharing arrangements.

2.8 Compliance with data protection law requires the ongoing commitment of everyone with a role in an organisation. This ranges from the individual's role in guarding against human error through to corporate level commitment to maintaining secure IT systems, organisation-wide training, and robust policies, advice and guidance on all aspects of data handling, including maintaining legally compliant and robust business processes. The Committee's role in supporting data protection compliance is to review the arrangements outlined in this report and make recommendations it deems necessary regarding prioritisation and implementation of changes needed to meet statutory requirements.

3. GENERAL DATA PROTECTION REGULATION (GDPR) REQUIREMENTS – TRANSPARENCY AND ACCOUNTABILITY

3.1 Data Protection law is underpinned by the key principles of transparency and accountability.

- The transparency principle means that information must be made available to customers about how and why their data is used, and data must be used fairly in accordance with that information. In the course of the year, privacy

notices across the Council, TfC and SCAS were reviewed and reissued to reflect changes to processing arrangements.

- The accountability principle makes the data controller responsible for complying with the UK GDPR. As controllers, the Council and its companies must be able to demonstrate their compliance with the overall requirements of GDPR and the Data Protection Act 2018 through the provision of documented evidence.

- Each controller is obliged to put in place appropriate technical and organisational measures to meet the accountability and transparency standards as well as the requirements of the data protection principles. To support these requirements the Council takes a 'Data Protection by Design' approach to the planning, implementation and management of business systems and operational arrangements. It is now mandatory to carry out a Data Protection Impact Assessment (DPIA) for high-risk initiatives and to seek advice from the Data Protection Office with regard to their completion. The purpose of the DPIA is to identify potential risks to individuals' data protection rights, and to consider how these can be negated or mitigated. The view of the DPO must be sought when preparing a DPIA and the organisation must document its views on the DPO advice provided and further record its mitigation and / or acceptance of residual risk.

3.2 During the 2022/23 financial year the Data Protection Office has supported the Council and its companies to develop 19 DPIAs for a range of projects, initiatives, and business process reviews. This has included ongoing involvement in a range of projects in partnership with the NHS, the ongoing deployment of Assistive Technology in Adult Social Care, initiatives under the Smart Cities agenda, and the development of the GOSS digital platform, which allows staff to provide real-time, interactive updates and feedback to customers about their requests for services or support.

3.3 Arrangements remain in place with ICT and Corporate Procurement to check that a DPIA has been considered before progressing activity; these have supported growing awareness of the requirement to seek DPO input. Outside these specialist areas, revised content and guidance on the Information Governance Service Hub continues to raise awareness of the requirement to consider DPIAs at the outset of any piece of business redesign, new initiative, or commissioning exercise.

3.4 A programme of compliance checks utilising the ICO's Accountability Framework was undertaken in 2022/23, covering Adult Social Care, Housing and Community Living, and Together for Children Sunderland.

3.5 The Accountability Tracker sets out a comprehensive series of compliance standards and controls across all aspects of the GDPR. 2022/23 checks focussed on key areas:

- Contracts and Data Sharing
- Data Protection by Design

- Data Subjects' Rights
- Transparency

3.6 All three service areas in scope of the checks demonstrated strong evidence of compliance, with most controls being fully or partially met. Where minor recommendations for improvement were identified, these were incorporated into the DPO Service Plan for 2023/24 for support and implementation.

3.7 The Council maintains e-learning for Elected Members and Council staff on the iLearn training platform. Both Elected Members and staff are expected to maintain their data protection knowledge using these modules. The DPO team receives monthly updates from the iLearn (and Me@TfC system for TfC) platforms on training completion.

4. SUBJECT ACCESS REQUESTS

4.1 One of the central rights given to individuals under GDPR and the Data Protection Act 2018 is for data subjects to have access to records containing their personal information. These requests continue to be coordinated on the Council's and TFC's behalf by the Access to Files team, a small specialist team of 3 officers, based in the Information Governance Team within the Corporate Support Service.

4.2 The Data Protection Office supported the Access to Files team with a review of process and procedure to check compliance given the changes in working requirements, with several recommendations being made. Amongst the recommendations made were changes to template correspondence and a recommendation to move from paper to electronic working, with the associated benefits in ensuring work carried out away from council premises is undertaken securely.

4.3 Outcomes for the year 1 April 2022 to 31 March 2023 are below.

2022/23	New cases received in Year	New cases closed in Year	New cases closed Within Timescale	New cases closed Out of Timescale	22/23 cases still open at 31/3/23
Total	**236**	**222 (94%)**	**136 (57%)**	**86 (37%)**	**14 (6%)**
Citywide	39	39	32	7	0
Adult SC	23	22	10	12	1
TfC	120	107	40	67	13
Blanks**	54	54	54	0	0

** Access to Files Team unable to establish Dept due to lack of proof of ID and/or clarification from the requestor. Requests are closed after 30 days. No requests for SCAS or Siglion in this period.

4.4 Members will note that of the 236 new cases closed in-year, 136 (57%) were responded to within the statutory timescale of one calendar month (three months for complex cases); 86 (37%) cases exceeded timescale, while 14 were still open at the end of the year – mostly cases received in February or March 2023.

4.5 This compares to 94 (52%) being in-time and 69 (39%) exceeding timescales in 2021/22. Given the substantial upturn in the number of new requests – 236 in 2022/23 against 180 in 2021/22 – this maintenance of performance under resource pressures can be substantially attributed to the changes to working practices, especially the adoption of new digital processes and the reversion to regular physical access to records held in City Hall.

4.6 It has historically proved challenging to respond within time-limits where a case involves multiple files/records - children's social care in particular, where a given case involves multiple family members, which often makes consideration of the interplay between individuals' privacy rights particularly complex. There is also a statutory requirement that Health and other professionals are asked for their view on the release of records originating from them and this can incur delays. The Access to Files Team continue to review working practices and explore technological options to improve the service offered.

5. INFORMATION INCIDENTS

5.1 A dedicated reporting email address ('Info Alert') is maintained for notifying data breaches directly to the Data Protection Office, to facilitate prompt recovery and containment actions by staff. A separate dedicated address is in place for use for similar reports made by Together for Children. SCAS have their own arrangements in place for reporting and investigating incidents. The Data Protection Office encourages reporting, not only of known or suspected breaches, but also the identification of lower level 'near miss' events. Such reports are used to inform recommendations for improvements that can be made before a 'near miss' puts the data protection rights of individuals at risk.

5.2 Appendix A details the numbers and gradings of breaches reported for the period from 1st of April 2022 to 31st March 2023. The Data Protection Office made use of a RAG rated matrix grading system to gauge the severity of reported breaches. Breaches rated Red meet the criteria for referral to the ICO. Appendix B provides information about the types and distribution of breach reports across the Council's Directorates and companies.

5.3 Common themes identified in previous annual reports remain apparent, these relate to:

- Correspondence errors, related to use of incorrect addresses (postal or email) or personal information of another incorrectly contained in correspondence sent to the correct address.
- Data quality issues frequently linked to, or proving to be the cause of, the above. Following management intervention the issue of re-use of previous

documents as templates was addressed and these instances declined for a period, although examples again occurred towards the end of the year.

5.4 Actions and recommendations taken/made include:

- Changes to business process and Team reminders about business process requirements.
- Staff involved in incidents refreshing their data protection training.
- Instructions to staff on following the correct process.
- Individual performance management.
- Double checking email and postal addresses and the contents of correspondence before sending.
- Use of clean templates for new documents.
- Requirement for e-mail data that is high risk or containing personal or sensitive information to be encrypted.

5.5 Arrangements for reporting data breaches are subject to ongoing review in the light of learning and feedback from incidents. The latest reporting materials are now published on the Information Governance Service Hub, providing for direct submission of reports to the Info Alert address, and giving staff instant access to breach management materials and advice for recovery, containment and investigation.

6. INFORMATION COMMISSIONER

6.1 No breaches were reported to the ICO in the course of the year

6.2 This compares with the previous year when four breaches were reported to the ICO.

7. COMPLIANCE ISSUES

7.1 A change to compliance monitoring was introduced in 2022/23, whereby compliance issues were captured. These are not personal data breaches where there has been a loss or unlawful disclosure of personal data but could be an infringement with any element of the GDPR. They are generally generated through:

- Customer complaints or allegations expressing dissatisfaction with how their data has been handled.
- A service area raising a query with the DPO Team, the nature of which suggests there may be a risk to compliance with the GDPR.
- Identification as part of the compliance checking programme.

7.2 Under Article 83 of the GDPR, an individual is entitled to seek compensation for material or non-material damage as a result of an infringement.

7.3 Appendix C details the numbers and categories of compliance issues in 2022/23. Members will note that 24 issues were recorded this year, with three key themes emerging:

- Customers complaining they did not consent to their data being shared, or that they were not made aware that their consent was not required as the basis to share.

- Complaints regarding the time taken to process Subject Access Requests

- Issues around Data Protection by Design, whereby DPIAs had not been undertaken, processor contracts or data sharing agreements with partner agencies were not in place.

8. THE CALDICOTT GUARDIAN ROLE AND THE ETHICS BOARD

8.1 The Caldicott Guardian (CG) is a senior person responsible for protecting the confidentiality of people's health and care information and making sure it is used properly. Within the Council, the role lies with the Performance Lead Manager for Adult Social Care in 2022/23.

The CG is supported by the Strategic Information Governance Group, which alongside its other functions acts as an Ethics Board to consider proposals for the use of personal information and make recommendations to the CG regarding the ethical and appropriate use of personal information.

8.2 Sunderland Care and Support and Siglion utilised the Council's Caldicott function in 2022/23, while in Together for Children the role is assigned to the Director of Children's Social Care.

9 NEXT STEPS

9.1 It is recommended that the Council and its connected organisations continue to engage with the Data Protection Office to refine arrangements for the use and management of personal data.

9.2 An ongoing programme of compliance checks, utilising the ICO's Accountability Framework, will continue into 2023/24, with periodic reports containing recommended actions for implementation being issued to Info Asset Owners.

9.3 Further embedding of 'Data Protection by Design' principles will be critical to ensure the DPO is involved at the earliest opportunity with new initiatives as the Council and partners move into the era of City Hall and to support the objectives of the City Plan. There are substantial implications for processing personal data posed by the Council's digitisation agenda underpinning programmes such as Smart City and City Hall.

9.4 The Government has tabled a Data Protection and Digital Information (DPDI) Bill which will modify some elements of the UK GDPR and Data Protection Act

2018. This bill has been through First and Second Readings and Committee and is currently at the Report Stage within the House of Commons. The Data Protection Office is monitoring progress of the Bill and will report to SIGG and Chief Officer Group when more detailed implications emerge.

10. RECOMMENDATIONS

10.1 The Committee is asked to consider the Data Protection arrangements in place, and performance against Data Protection standards in the 2021/22 year and provide its comments on the information provided in this report.

11. REPORT CONTACT

Nick Humphreys
Data Protection Officer
nick.humphreys@sunderland.gov.uk

APPENDIX A

Number reported 2021/22	Reporting Measure	Measure Description	Number reported 2022/23
1	ICO Reported	Number of personal data breaches reported to the ICO	0
3	ICO report - Council	Number of breaches self-reported to the ICO	0
1	ICO report - Public	Number of customer reports to the ICO by a member of the public alleging a personal data breach.	0
96	**Breach Total**	**The total number of cases where a report or request for advice has identified a Personal Data Breach**	**58**
3	Red	Number of cases where a personal data breach via SIRI - Serious Incidents Requiring Investigation - Red Rating	0
9	Amber	Number of cases where a personal data breach has been reported or identified via SIRI - Serious Incidents Requiring Investigation - Amber Rating	4
66	Green	Number of cases where a personal data breach has been identified via SIRI - Serious Incidents Requiring Investigation - Green Rating	54
18	Data Protection Issue (non-breach)	Data Protection issue (non-Article 4 of GDPR, i.e. concluded **not** a data breach after investigation)	N/A Now recorded as compliance issue (see Appendix C)

APPENDIX B

Breach Type by Directorate	Disclosed in Error	Lost in Transit	Process Not Followed	Technical Failure	Other	Total
City Development	2				2	**4**
Corporate Services	11		2	1	1	**15**
Neighbourhoods	11			1	2	**14**
Public Health	1		1			**2**
SCAS						**0**
Siglion			1			**1**
Together for Children	15		5			**20**
Universal	1			1		**2**
Total	**41**		**9**	**3**	**5**	**58**

APPENDIX C

Compliance Issue Type Directorate	No lawful basis to process info	Inaccurate data being processed	Individuals' rights not being recognised (SARs)	Data Protection by Design not considered	Total
City Development					
Corporate Services	1		7	1	**9**
Neighbourhoods			2		**2**
Public Health				1	**1**
SCAS					
Siglion					
Together for Children	2	1	6		**9**
Universal			3		**3**
Total	**3**	**1**	**18**	**2**	**24**