Sunderland City Council

Item No. 9

AUDIT AND GOVERNANCE COMMITTEE **22 July 2022**

DATA PROTECTION – ANNUAL REPORT 2021/22

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 2021/22 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 DP compliance from the Council's Data Protection Office, a Strategic Information Governance Group made up of senior officers and chaired by the Executive Director for Corporate Services 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, NECA and those schools and academies which subscribe to the service.

2.2 Following the appointment of a new DPO in March 2021, 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 direct advice and guidance to support IAOs and service areas with DP compliance during this transitional

period. During 2021/22, the DPO team has been part of the Corporate Support Review, 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' in line with the Thinking Operating Model.

2.3 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. 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.

2.4 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 both regularly scheduled and ad-hoc information sharing arrangements.

2.5 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 deliver on corporate requirements.

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

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

- The transparency principle means that information must be made available to data subjects 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 provided to customers have been 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 requirements of transparency in addition to 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 2021/22 financial year the Data Protection Office has supported the Council and its companies to develop 18 DPIAs for a range of projects, initiatives, and business process reviews. This has included ongoing involvement in a range of public health programmes to support Covid responses, the roll-out of Assistive Technology in Adult Social Care, CCTV deployment under the Smart Cities agenda, and development of a Mobility Hub platform.

3.3 Arrangements remain in place with ICT and Corporate Procurement to check that a DPIA has been considered before progressing; these have supported growing awareness of the requirement to seek DPO input. Outside these specialist areas, use of 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 There remains a requirement for service areas to maintain a Record of Processing Activity (ROPA) for all business activities involving personal data, to support the accountability principle. In preparation for GDPR implementation in 2018, service areas each completed a self-assessment to evaluate and record their compliance arrangements. DPO team members undertook a significant piece of work to develop and pre-populate a bespoke ROPA template based on the ICO's best practice, with the information from the self-assessment returns.

3.5 A work programme planned for 2020/21 for each service area to review and update their ROPA templates, essentially with further information identified by the ICO, was postponed due to Covid priorities. A new programme, providing support to service areas while aligning with agile working arrangements, is incorporated into a programme of compliance checks in 2021/22.

3.6 The Council maintains e-learning for Elected Members and Council staff on the learning hub. Both Elected Members and staff are required to maintain their data protection knowledge using these modules. The DPO team receives monthly updates from People Management 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 Business Support.

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 imposed by Covid, 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 2021 to 31 March 2022 are below.

2021/22	Received in Year	Closed in Year	Closed Within Timescale	Closed Out of Timescale	Remain open
Total	**180**	**163 (91%)**	**94 (52%)**	**69 (39%)**	**17 (9%)**
Citywide	24	23	15	8	1
Adult SC	11	9	5	4	2
TfC	101	87	30	57	24
Blanks**	44	44	44	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 163 cases closed in-year, 94 were responded to within the statutory timescale of one calendar month; 69 cases exceeded timescale. This compares to 61 being in-time and 79 exceeding timescales in 2020/21. This upturn 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, previously unavailable due to lockdown.

4.5 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 delay. The ICO Office has taken a pragmatic view of the matter, especially under Covid arrangements, but is taking a keener interest in timescales when customers have registered a complaint with them. 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 2021 to 31st March 2022. 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 the previous annual report remain apparent, these relate to:

- Correspondence errors, related to use of incorrect addresses (postal, text or email) or personal information of another incorrectly contained in correspondence sent to the correct address.
- Dissatisfaction with data sharing within the safeguarding process.
- 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.
- 'Orphan' records following re-organisation and the departure of the staff responsible for the service. This represents an 'availability' breach where the location of the records is not properly understood.

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.
- Introduction of 100% checks of correspondence.
- 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 to mitigate the risks.
- Review of records held and to be retained for future use, with secure destruction arrangements in place where documents are not required to be retained.

5.5 Arrangements for reporting data breaches are subject to ongoing review in the light of learning and feedback under the Corporate Support Review. The latest reporting materials are now published on the Information Governance Service Hub, providing for direct submission of reports to the Info Alert address. Based on feedback from users it is recognised that, through effective use of triage, these arrangements can now be further refined, while continuing to gather sufficient data to provide an effective picture of where practice issues may compromise data protection and/or expose the Council.

6. INFORMATION COMMISSIONER

6.1 Four breaches were reported to the ICO in the course of the year; three by the Council and one by a member of the public.

The public complaint was reported after internal Council investigations were unable to substantiate allegations of personal information being inappropriately disclosed in relation to a planning application.

The Council reported three breaches directly to the ICO:

- Two cases around children's safeguarding, where parental addresses were disclosed to estranged family members without a legitimate basis to do so
- One case of missing paper records highlighted during the bulk migration of paper records from the Council's Records Management contractor to a new provider.

6.2 This compares with the previous year when one breach was reported to the ICO.

6.3 There has been no formal enforcement action taken in relation to the above breaches, or with the Council's and its connected organisations' general compliance with their data protection responsibilities. Where the ICO has made

recommendations these have been accepted and implemented within the service areas.

8. PROJECT SUPPORT

8.1 Windows 10 / Office 365

The Data Protection Office has continued work to support the development and roll-out of the suite of products under Windows 10 and Office 365, with representation on the W10/365 Strategic Governance Group and the Strategic Management Information Security Forum (MISF), providing specialist advice on data protection aspects and on anticipated issues with deployment. DPO advice has been provided on the mitigating measures identified through the Project DPIA documents; however, the 'evergreen' nature of the Office 365 environment means that ongoing changes and updates to functionality continue to require Data Protection Office input. Due to Covid and the need for staff to principally work from home there was a need to rapidly roll-out the availability of Teams (and its modules) including provision of guidance to staff on its use. The Data Protection Office will continue to work with the ICT service with regard to the implementation of additional functionality.

8.2 City Hall, Agile Working and Civic Centre

The Data Protection Office supported the developing proposals for the design and occupation of City Hall and the agile working arrangements inherent to it, and also the closure of the Civic Centre, with particular emphasis on the migration, archiving or secure disposal of both paper and electronic records.

9. THE CALDICOTT GUARDIAN ROLE AND THE ETHICS BOARD

9.1 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 lay with the Executive Director of Neighbourhoods in 2021/22.

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.

9.2 Sunderland Care and Support and Siglion utilise the Council's Caldicott function, while in Together for Children the role is assigned to the Director of Children's Social Care.

10 NEXT STEPS

10.1 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.

10.2 An ongoing programme of compliance checks, utilising the ICO's Accountability Framework, will continue into 2022/23, with quarterly reports containing recommended actions for implementation being issued to Info Asset Owners.

10.4 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, City Hall, and the Corporate Support Review.

10.5 The Data Protection Office has developed a revised Service Plan for 2022/23 to capture work to support the above. The plan builds on the IMPS and Corporate Support Review to implement a suite of Data Protection Protocols in areas like Breach Management, People's Rights, and Data Protection by Design, while an updated Performance and Reporting Framework for 2022/23 shifts the emphasis away from recording lower-level data breaches and reflects the emerging requirement to monitor compliance concerns raised by members of the public or highlighted in the programme of checks.

11. RECOMMENDATIONS

11.1 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.

12. REPORT CONTACT

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

APPENDIX A

Number reported 2020/2021	Reporting Measure	Measure Description	Number reported 2021/22
1	ICO Reported	Number of personal data breaches reported to the ICO	4
1	ICO report - Council	Number of breaches self-reported to the ICO	3
0	ICO report - Public	Number of customer reports to the ICO by a member of the public alleging a personal data breach.	1
136	**Breach Total**	**The total number of cases where a report or request for advice has identified a failing in Data Protection compliance**	**96**
0	Red	Number of cases where a personal data breach via SIRI - Serious Incidents Requiring Investigation - Red Rating	3
34	Amber	Number of cases where a personal data breach has been reported or identified via SIRI - Serious Incidents Requiring Investigation - Amber Rating	9
86	Green	Number of cases where a personal data breach has been identified via SIRI - Serious Incidents Requiring Investigation - Green Rating	66
16	Data Protection Issue (non-breach)	Data Protection issue (non-Article 4 of GDPR, i.e. concluded **not** a data breach after investigation)	18

APPENDIX B

Breach Type by Directorate	Disclosed in Error	Lost in Transit	Process Not Followed	Technical Failure	Other	Total
City Development	2				1	**3**
Corporate Services	19		4	1		**24**
Neighbourhoods	17		2			**19**
Public Health						**0**
SCAS	1		1			**2**
Siglion						**0**
Together for Children	38		4	1		**43**
Universal	4		1			**5**
Total	**81**		**12**	**2**	**1**	**96**