Sunderland City Council

Item No. 10

AUDIT AND GOVERNANCE COMMITTEE **26 July 2019**

DATA PROTECTION – ANNUAL REPORT 2018 – 2019

Report of the Director of People, Communications and Partnerships and 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:

(i) Data Protection arrangements outlined in this report
(ii) Performance against Data Protection standards in the 2018-19 year.
(iii) Comments and issues the Committee would highlight to the Council's leadership team.

2. Background

2.1 The Council is required to appoint a Data Protection Officer to advise on its data protection responsibilities and act as its point of contact with the Information Commissioner's Office. The Council's Data Protection Officer has been appointed and the Council receives wider support with DP compliance from the Council's Data Protection Office. 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 This report appraises the Committee of arrangements and performance with regard to Data Protection (DP) compliance and performance following implementation of the General Data Protection Regulation and Data Protection Act 2018 This legislation replaced the Data Protection Directive 1995, and the Data Protection Act 1998 in the UK with effect from 25 May 2018**.**

2.3 As a data controller, the Council is required to pay an annual fee and is registered as a fee payer with the Information Commissioner's Office, as

are Together for Children and Sunderland Care and Support. 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 and retain all the associated data protection responsibilities. The Council also acts as data processor for the other organisation in relation to some of the information it processes, 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, and standard contract clauses have been incorporated to reflect current Data Protection requirements of processors.

2.4 Compliance with the data protection regime requires the commitment of every function within a corporate organisation. It is recognised that data protection breaches are commonly caused by internal human error rather than external attack, although this too presents a risk to data. This requires implementation and maintenance of secure IT systems, organisation-wide training and robust policies on all aspects of data handling. DPA breaches only occur when a business process has either not been followed properly, or the process wasn't DP compliant in the first place. The role of the Committee in this context is to review the arrangements outlined in this report and make recommendations to the Council regarding prioritisation and implementation of changes needed to deliver on data protection requirements.

3. GDPR REQUIREMENTS – TRANSPARENCY AND ACCOUNTABILITY

3.1 The new data protection laws are underpinned by the two key principles of transparency and accountability. Requirements for transparency data to be made available to data subjects have been re-framed and a significant piece of work was undertaken in preparing for GDPR to identify where and how personal data is held and used within the Council, to feed into the preparation of information for service users, employees and others, about how their data is used.

3.2 The accountability principle requires the Council, as a data controller, to have

> "appropriate technical and organisational measures in place" to adopt the data protection principles, and to be able to demonstrate this. To support this data controllers must adopt a 'privacy by design' approach to the management of business systems and operational arrangements. Where previously it was recommended good practice to carry out Data Protection Impact Assessments (DPIA) to identify how risk to data can be planned out and/or mitigated, primarily for high risk

initiatives, this is now mandatory in designated circumstances. The value of the DPIA lies in bringing attention to potential risk to privacy rights from the start of a project or initiative, with participants pooling knowledge and expertise to identify solutions that minimise and mitigate potential risks. The view of the DPO must be sought when preparing a DPIA and the business must document its views on the DPO advice provided and document its acceptance of residual risk.

3.3 The 2018-19 year has seen the Council and its companies develop DPIA for numerous projects, initiatives and business process reviews. Areas reviewed include elements of the Office 365/Windows 10 project, proposals for use of drones in the planning environment, use of assistive technologies in the homes of elderly or disabled adults, use of CCTV on refuse lorries, the Step up Sunderland initiative,), support for women with multiple pregnancies, procurement of supported accommodation, use of i-pads to obtain children's views and the Sunderland SEND (hybrid mail) project.

3.4 Arrangements have been put in place to check DPIA has been considered before progressing developments in ICT or procurement and the checks in place have successfully directed lead officers to seek DPO input. In the context of the wide range of processing activity across services there are, however, likely to be many other areas that would benefit from review with regard to data risk and mitigations and it is recommended that attention is given to raising awareness of the requirement to consider DPIA at the outset of any piece of business redesign or commissioning.

4. SUBJECT ACCESS REQUESTS

4.1 One of the central data subject rights under GDPR and the Data Protection Act 2018 is to have access to records containing their personal information. These requests are coordinated on the Council and Company behalf by the Access to Files team within the council's Business Support service. This is a small specialist team of 4 officers, based in the Information Governance Team.

4.2 This team previously handled only those requests related to Childrens and Adults records. With implementation of GDPR the team took on the additional role of coordinating responses to all Subject Access requests received across council services. This work was absorbed within existing resources

4.3 Outcomes for the year 25 May 2018 (GDPR implementation) and 1 June 2019 are below. Future reports will provide these statistics reporting annually 1 June to 31 May.

	Open at 25/5/15	Received in year	Closed in year	Within timescale	Outside timescale
Total	32	163	172	147	25
Council	n/a	44	36	35	1
TfC	32	119	136	112	24

4.4 Members will note that of the 172 cases closed in-year 147 were responded to within the statutory timescale of 1 calendar month, which may be extended up to 3 calendar months in the case of complexity or multiple requests. The timescale for reply was previously 40 days. 25 cases exceeded timescale, 24 TfC and 1 Council. It has historically proved challenging to respond within time-limits where a case involves multiple files/records, in particular where a childrens' case involves multiple family members. There is also a requirement that Health and other professionals are asked for their view on release of records originating from them and this can incur delay.

5. INFORMATION INCIDENTS

5.1 A dedicated reporting address ('info.alert') for incidents and concerns about data protection compliance which routes reports direct to the Data Protection Office was established to promote prompt reporting by staff. A separate dedicated address is in place for use for reports made to the Data Protection Office by Together for Children. The Data Protection Office encourages reporting, not only of known or suspected breaches, but also the identification of low-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 Monthly performance reports enable senior management to monitor trends and highlight issues in relation to reports made to the info.alert address. Appendix A details the number of breaches reported for the period from 1st of June 2018 to 31th of May 2019. The Data Protection Office makes use of a RAG rated matrix grading system aligned to that in use within health services to allocate reports of breach. Appendix B provides information about breach ratings and the distribution of breach reports across the Council's Directorates and companies.

5.3 Common themes 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/cause of the above, including through re-use of previous documents as templates

- Abandoned files and documents abandoned on printers
- '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.

Action taken includes;

- 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 operational where documents are not required to be retained.

5.4 Learning from cases feeds into business improvement, and a focused piece of work was undertaken by the Data Protection Office looking into the origin of addressing errors that resulted in misdirection of post and related incidents. Recommendations include;

- A prompt response to an incident, including early investigation to establish the background facts, is a critical factor in containing the incident and mitigating the risk of harm to data subjects.
- As soon as a data breach is identified priority should be given to remedying the breach and mitigating its consequences as quickly as possible. Formal documented notification is of lower priority than identifying the immediate practical steps that can be taken. Generally, where for example, the recipient reports they have received correspondence in error, the first step should be to go out and retrieve it, making sure the recipient understands it can be an offence to make use of any information they may have read. Response, containment and reporting of such incidents must be prioritised accordingly.
- Having contained the incident it is important to progress investigation of the cause to its conclusion and identify the measures to be put in place to prevent recurrence, assigning responsibility for implementation and a timescale for completion, these are monitored centrally through the DP Office.
- Sunderland SEND (Hybrid Mail) is not a complete solution to postal errors – the new arrangements can only ever be as good as the raw data it receives: there should be review & update of QA arrangements for data accuracy in recordkeeping systems and in work completed, in order to strengthen compliance with GDPR accuracy, relevance & currency requirements.

- ‘Human Errors’ are not usually unavoidable – where the same ‘error’ occurs there should be a review of the adequacy of skills, training and capacity of staff involved and the business process they’re following.

5.5 Data breach reporting arrangements have been reviewed and simplified in the light of learning and feedback during this first year of operation of the DPO arrangements and are to be embedded in the revised intranet being designed within Office 365 to improve efficiency through direct submission of the reporting template to the info.alert address.

6. INFORMATION COMMISSIONER

6.1 Seven breaches were reported to the Information Commissioner in the course of the year. Of these four were reported by the Council and three by members of the public.

- A birth certificate sent to the address of a third party unrelated to the data subject. The ICO found that there has been an infringement due to human error and have made recommendations that could lower the likelihood of a similar incident occurring.
- An unauthorised access to library services software. The contractor reported that some 45 customers’ personal data was accessed. The ICO recognised the incident as a cyber breach and came to the decision not to take any formal enforcement action due to the nature of the case and the remedial measures put in place on the recommendation of the DPO.
- An acknowledgement letter intended for the complainant was included in correspondence sent to the subject of the complaint. The breach was caused by human error. The ICO has recommended the Council review its processes, and confirmed they will take no further action on the case.
- Inclusion of an address in a court report, where it was alleged this may pose a risk of renewed domestic violence. Once provided with detailed background information the ICO concluded this had not been a reportable breach.
- Publication of a private telephone number as part of a contacts list. The ICO found this was a breach and procedures have been amended to address the risk of recurrence.
- Sharing information about the data subject’s convictions in the context of safeguarding concerns. The ICO did not find an infringement
- Sharing information with a neighbouring authority. The ICO initially found no infringement, but subsequently reviewed the case and concluded information had not been shared appropriately.

6.2 There has been no formal enforcement action taken in relation to the Council's, or its connected organisations' compliance with their data protection responsibilities. The ICO has however made practice recommendations in relation to cases reported to her office and these have been accepted and implemented.

7. REGULATION OF INVESTIGATORY POWERS ACT

7.1 Oversight of the Council's use of covert surveillance was allocated to the Data Protection Office with effect from April 2019. There has been no use of RIPA authorisation since that date. Specialist training attended by members of the Data Protection Office, Authorising Officers and service lead officers took place on 19th July 2019.

8. NEXT STEPS

8.1 It is recommended that the Council and its connected organisations continue to work with the Data Protection Office to refine arrangements in the light of the first year's operation of GDPR. Transparency information, policies and procedures will go through an annual review, to be aligned with requirements identified during the year. Elected Members and staff should also be required to complete annual refresher training, using the updated e-learning package which will shortly be available.

8.2 In preparation for the Council moving to City Hall and adopting a digital by default approach to record-keeping, a programme is underway to identify and destroy or re-locate paper records, as appropriate according to the stage they have reached in the record lifecycle. This exercise includes review and updating of retention schedules for staff to implement. An audit of records will provide the information that is needed to consider the business case for archiving or digitisation of those records that must be retained.

8.3 A programme of review of data use in preparation for GDPR provided the baseline to demonstrate commitment to the accountability principle. A further review is now required, to provide a current record of information asset processing activity (ROPA).

9. RECOMMENDATIONS

9.1 The Committee is asked to consider the Data Protection arrangements in place, performance against Data Protection standards in the 2018-19 year and provide its comments on the information provided in this report.

10. REPORT CONTACT

Rhiannon Hood
Data Protection Officer
rhiannon.hood@sunderland.gov.uk
0191 561 1005

APPENDIX A

LPI Number	Compliance issues	Measure Description	Number Received 1 June 2018 - 31 May 2019
1019	ICO Reported	Number of personal data breaches reported to the Information Commissioners Office (ICO)	7
1019a	ICO report Civic	Number of breaches self-reported to the Information Commissioners Officer (ICO)	4
1019b	ICO report Public	Number of customer reports to the Information Commissioners Officer (ICO) by a member of the public alleging a personal data breach.	3
1267	Breach Total	The total number of cases where a report or request for advice has identified a failing in Data Protection compliance	170
1259a	Red	Number of cases where a personal data breach via SIRI - Serious Incidents Requiring Investigation - Red Rating	4
1259b	Amber	Number of cases where a personal data breach has been reported or identified via SIRI - Serious Incidents Requiring Investigation - Amber Rating	50
1259c	Green	Number of cases where a personal data breach has been identified via SIRI - Serious Incidents Requiring Investigation - Green Rating	105
1281	Compliance Issue (non-breach)	Data Protection Compliance issue (non-article 4)	11