Appendix

AUDIT AND GOVERNANCE COMMITTEE **24 July 2020**

DATA PROTECTION – ANNUAL REPORT 2019 - 2020

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:

- Data Protection arrangements outlined in this report
- Performance against Data Protection standards in the 2019-20 year.
- Comments and issues the Committee would highlight to the Council's senior leadership.

2. Background

2.1 The Council has appointed the Data Protection Officer (DPO) as required by data protection law, to advise on its data protection responsibilities and act as its point of contact with the Information Commissioner's Office. The Council receives 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 Strategic Director of People Communications and Partnerships in the role of Senior Information Risk Officer (SIRO), and an Operational Information Governance group of operational managers chaired by the DPO. The work of these groups feeds into Directorate working arrangements. 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 NELEP and those schools and academies which subscribe to the service.

2.2 This is the second annual report provided to inform 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. The first annual report was based on full-month data running from the date of implementation of GDPR on 25 May 2018 to 1 June 2019. The reporting period is now aligned with the Council year and data provided relates to the year 1 April 2019 to 31 March 2020. Future annual reports will follow the same principle.

2.3 As a data controller, the Council remains obliged 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. Schools and Academies are also required to pay the annual fee as individual concerns. 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, and standard contract clauses have been incorporated to reflect current Data Protection requirements of processors.

2.4 Increasingly the Council and its companies work in partnership with other organisations, including other Councils, Health partners and Voluntary and Community Services under both formal and informal information sharing arrangements.

2.5 As reported in the first annual report, compliance with data protection law requires the 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 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 to the Council regarding prioritisation and implementation of changes needed to deliver on corporate requirements.

3. 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 their data is used, and data must be used fairly in accordance with that information. In the course of the year information provided to customers has been reviewed and developed to reflect changes within the organisations and the suite of council policies and procedures reviewed for reissue.

3.2 The Accountability data protection principle makes the data controller responsible for complying with the GDPR. This means the Council and its companies must be able to demonstrate their compliance with the overall requirements of GDPR and the Data Protection Act 2018. Each data 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 'privacy 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 business must document its views on the DPO advice provided and document its mitigation and / or acceptance of residual risk.

3.3 During 2019-20 year the Data Protection Office has supported the Council and its companies to develop DPIA for a range of projects, initiatives and business process reviews. This has included ongoing involvement in advising on elements of the Office 365/Windows 10 project, a range of public health initiatives, Council initiatives including proposals for the use of drones, remote monitoring of fly tipping sites, and sharing information with partners in support of a range of health and other initiatives.

3.4 Arrangements remain in place to check that DPIA has been considered before progressing developments in ICT or procurement and have supported growing awareness of the requirement to seek DPO input. Outside these specialist areas, use of the service hub and communications have continued to raise awareness of the requirement to consider DPIA at the outset of any piece of business redesign or commissioning.

3.5 In support of the Accountability principle a Record of Processing Activity (ROPA) is required for all business activities relying on personal data processing. In preparation for GDPR implementation, service areas each completed a self-assessment to evaluate and record their compliance arrangements. This has been translated into ROPA format based on requirements and best practice recommended by the ICO's office. Two team members have undertaken a significant piece of work to develop and pre-populate a bespoke ROPA template for council and company use. This is in a format that auto populates data controller responsibilities in relation to the data subject rights which flow from the legal basis for the processing undertaken by each business area. They have also worked to pre-populate the template for service areas based on the information gathered through the self-assessments. The resulting pre-populated templates now require review and updating by each service area to add further information identified by the ICO and update existing information to ensure each ROPA reflects up to date information about the arrangements, processes, procedures and systems currently in use for managing data in the service area. The ROPA, like the DPIA, is a 'living

document' that needs periodic review to maintain its currency and relevance.

3.6 In the course of the year the council participated in a local authority collaboration to develop e-learning for Elected Members and this together with an updated e-learning package for staff has been published to the learning hub. Both Elected Members and staff are required to bring their data protection knowledge up to date using these updated modules. Refresher training will then be made available in future for those who have completed these, allowing Members and staff to update and maintain their knowledge efficiently and effectively to meet the expectations of the Information Commissioner's office and the requirements for sharing data with Health and other partners.

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 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 within Business Support.

4.2 During the year the Data Protection Office supported the Access to Files team with a review of process and procedure to audit compliance with changes in the subject access requirements introduced with GDPR and the Data Protection Act 2018, 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 I April 2019 and 31 March 2020 are below.

	Open at 25/4/19	Received in year	Closed in year	Within timescale	Outside timescale
Total	8	147	144	95	49
Council(*)	1	45	47	33	14
*SCAS	*1	*11	*11	*4	*7
TfC	7	102	97	62	35

4.4 Members will note that of the 144 cases closed in-year 95 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. 49 cases exceeded timescale, 35 TfC and 14 Council.

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 requirement that Health and other professionals are asked for their view on release of records originating from them and this can incur delay. This is an issue faced by many local authorities and where best endeavours can be shown (as in SCC), the Information Commissioners Office has taken a pragmatic view of the matter. Nonetheless, Access to Files continue to review working practices to improve the service offered.

5. INFORMATION INCIDENTS

5.1 A dedicated reporting address ('info.alert') is maintained where incidents and concerns about data protection compliance are routed directly to the Data Protection Office, to facilitate prompt reporting by staff. A separate dedicated address is in place for use for similar 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 Appendix A details the numbers and gradings of breaches reported for the period from 1st of April 2019 to 31st March 2020. The Data Protection Office makes use of a RAG rated matrix grading system aligned to that in use within health services to gauge the severity of reported breaches. Breaches rated Red meet the criteria for referral to the ICO and are also reported monthly to the performance clinic. 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 cause of the above. Following management intervention within TfC 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.

- 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.

5.4 Actions and recommendations 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 operational where documents are not required to be retained.

5.5 Arrangements for reporting data breaches were reviewed and simplified in the light of learning and feedback during the first year of operation of the DPO arrangements, and are now embedded in the Data Protection materials on the Service Hub providing for direct submission of the reporting template 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 Five breaches were reported to the Information Commissioner in the course of the year. Of these four were reported by the Council and one by the external provider of their system, in use nationally, that was thought to have been breached. This compares with the previous year when seven breaches were reported to the Information Commissioner, four being reported by the Council and three by members of the public. In 2019-20 these five breaches related to;

- A breach of security within the library management system, reported to the ICO and the council by the system provider.

- Identification of a complainant to the person complained about through misdirection of a letter responding to the complaint.
- Unauthorised access by a council employee to personal data of individuals held in a management system.
- Release of information about one young person to another.
- Misdirection of a letter concerning family circumstances to a neighbour.

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 indicated they are considering whether to take action against a former employee in one case and has made practice recommendations to the Council in relation to other cases reported to her office. These recommendations have been accepted and implemented. In relation to the remaining case, while the practice recommendations have been accepted and implemented the council and TfC have placed on record their disagreement with other aspects of the ICO's findings, setting out detailed reasons for this.

7. SUPPORT TO THE COVID 19 RESPONSE

7.1 Towards the end of the year the Data Protection Office supported the council and partners in implementing data sharing arrangements in response to the COVID 19 pandemic against a changing set of requirements, guidance and legislation including the Coronavirus Act 2020 which received Royal Assent on 25th March. The ICO has issued guidance specifically concerning COVID matters. Government has also issued Directions in relation to many aspects of management of the pandemic, including on sharing data about vulnerable individuals requiring support from local authorities. There have also been requirements for Data Protection Office advice from other clients including schools and academies regarding management of personal data for the purpose of supporting individuals and schools attendance.

7.2 As a consequence of the pandemic Council services have needed to respond flexibly to maintain very high levels of service to our customers, including the deployment of new technologies, the quick modification of processes and the movement of many officers to work from home during this period. The Data Protection Office has (in line with the Information Commissioner's position on flexibilities during the crisis) provided advice and guidance in response to the current situation, seeking to identify and mitigate the highest risks as and where possible while supporting the flexibilities that circumstance has demanded. These changes have necessarily been made at pace without the full level of evaluation of all

potential data protection impacts that the Council would ordinarily be required to take. Where it is proposed to maintain new arrangements in whole or in part, the usual requirement to carry out a Data Protection Impact Assessment (DPIA) in relation to technical or organisational change will need to be applied and identified mitigations will need to be implemented. This may present a significant workload for services and the Data Protection Office during the post-Covid period, if the changes are numerous and impact on the management and use of personal data.

8. OTHER PROJECT SUPPORT

8.1 GREAT NORTH CARE RECORD

During the year a Data Protection Office lead has supported development of information sharing arrangements to form the Great North Care Record (GNCR) working in partnership with colleagues from Health and other local authorities. The GNCR covers the 3.6 million people living in the North East and North Cumbria and will provide a readily accessible route to share patient information securely between health and care staff. This will allow staff to access individuals' most current health details from all sources, providing a holistic, up to date and immediate view of each patient's health status and needs. In response to the COVID 19 emergency, arrangements are being developed to reflect the data sharing arrangements introduced to support the national response. These arrangements will be substituted with business as usual arrangements once the current measures are withdrawn.

8.2 OFFICE 365

The Data Protection Office has continued work to support implementation of Office 365, with representation on the Project Board and Centre of Excellence working group, commenting and providing specialist advice on the data protection aspects and on anticipated issues with implementation. Data Protection Officer advice has been provided on the mitigating measures identified through the Project Data Protection Impact Assessment documents and the 'evergreen' nature of the Office 365 environment means that ongoing changes and updates to functionality will require similarly ongoing Data Protection Office input. Latterly the rapid implementation of Teams in order to address COVID 19 emergency issues, primarily the need to rapidly equip staff to work remotely, has not facilitated detailed evaluation of each element of functionality as had been recommended and planned. As above, these considerations will be revisited in due course as and when the COVID 19 situation allows a return to more proactive than reactive planning and deployment.

8.3 City Hall

The Data Protection Office has supported the developing detailed proposals for the design and occupation of City Hall, recruiting an intern from University of Sunderland to provide support to preparatory arrangements for reducing the volume of paper records to be transferred into City Hall, with a programme of records 'weeding' and destruction, and advising on transfer to electronic storage. Advice has also been provided in support of DPIA of the proposed arrangements.

9. The Caldicott Guardian Role and the Ethics Board

9.1 It has been notable in the past year that, while materials to support consultation with the Caldicott Guardian on ethical matters is available, its use for formal consultation with the Caldicott Guardian has not been evident. Following a review of arrangements by the DPO the Strategic Information Governance Group considered the question of support for the Caldicott Guardian role and recommends that the Group take on the additional role of Ethics Board, to consider proposals for use of personal information and make recommendations on these to the Council's Caldicott Guardian, the Executive Director of Neighbourhoods, regarding the ethical and appropriate use of personal information. Sunderland Care and Support utilise the Council's Caldicott function and in Together For Children the role is assigned to the Director of Children's Social Care.

The Caldicott Guardian Council outlines the responsibilities of the role in its Manual for Caldicott Guardians as follows;

Strategy & governance: the Caldicott Guardian should champion confidentiality issues at Board/senior management team level, should sit on an organisation's Information Governance Board/Group and act as both the 'conscience' of the organisation and as an enabler for appropriate information sharing.

Confidentiality & data protection expertise: the Caldicott Guardian should develop a strong knowledge of confidentiality and data protection matters, drawing upon support staff working within an organisation's Caldicott and information governance functions, but also on external sources of advice and guidance where available.

Internal information processing: the Caldicott Guardian should ensure that confidentiality issues are appropriately reflected in organisational strategies, policies and working procedures for staff.

Information sharing: the Caldicott Guardian should oversee all arrangements, protocols and procedures where confidential personal information may be shared with external bodies and others with

responsibilities for social care and safeguarding. This includes flows of information to and from partner agencies, sharing through IT systems, disclosure for research, and disclosure to the police.

Many or all of these responsibilities may be shared with the Senior Information Risk Officer (SIRO), with whom the Caldicott Guardian should work closely.

Staff should be advised to seek assistance from the Caldicott Guardian where necessary; typical examples of such situations are:

- a request from the police for access to people's information;
- requests from patients to delete their records;
- an actual or alleged breach of confidentiality.

10. REGULATION OF INVESTIGATORY POWERS ACT

10.1 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, or indeed several years previously. Specialist training attended by members of the Data Protection Office, Authorising Officers and service lead officers took place on 19th July 2019. A formal inspection by IPCO in November 2019 concluded in relation to the Council's arrangements that; -

> **'Whilst it [the Council] has also undergone a significant internal transformation in 2019 in terms of departments and senior officers, it has retained key people in place to oversee and, if necessary, authorise covert tactics. The training materials and policy documents are very good and Members appear to be very well informed. The discussions during the inspection showed a high level of understanding about privacy, human rights and the difference, and occasional fine line, between overt and covert surveillance. There are some innovative developments on the technical equipment front, all of which have been afforded due consideration about the privacy implications before roll-out.**"

11. NEXT STEPS

11.1 It is recommended that the Council and its connected organisations build on their engagement with the Data Protection Office to refine arrangements for the use and management of personal data in the light of shared experience of implementation of the revised data protection legislation to date.

11.2 Services' engagement in review of the information pre-populated to the ROPA for their area is essential and proceeding. This will provide a current record of information asset processing activity as required under GDPR.

11.3 Awareness raising and compliance checks in support of the Caldicott Guardian role will be necessary to ensure the Caldicott Guardian's view on implementation of initiatives is engaged at the appropriate point for all proposals that raise ethical issues in relation to the use of personal data.

12. RECOMMENDATIONS

12.1 The Committee is asked to consider the Data Protection arrangements in place, and performance against Data Protection standards in the 2019-20 year and provide its comments on the information provided in this report.

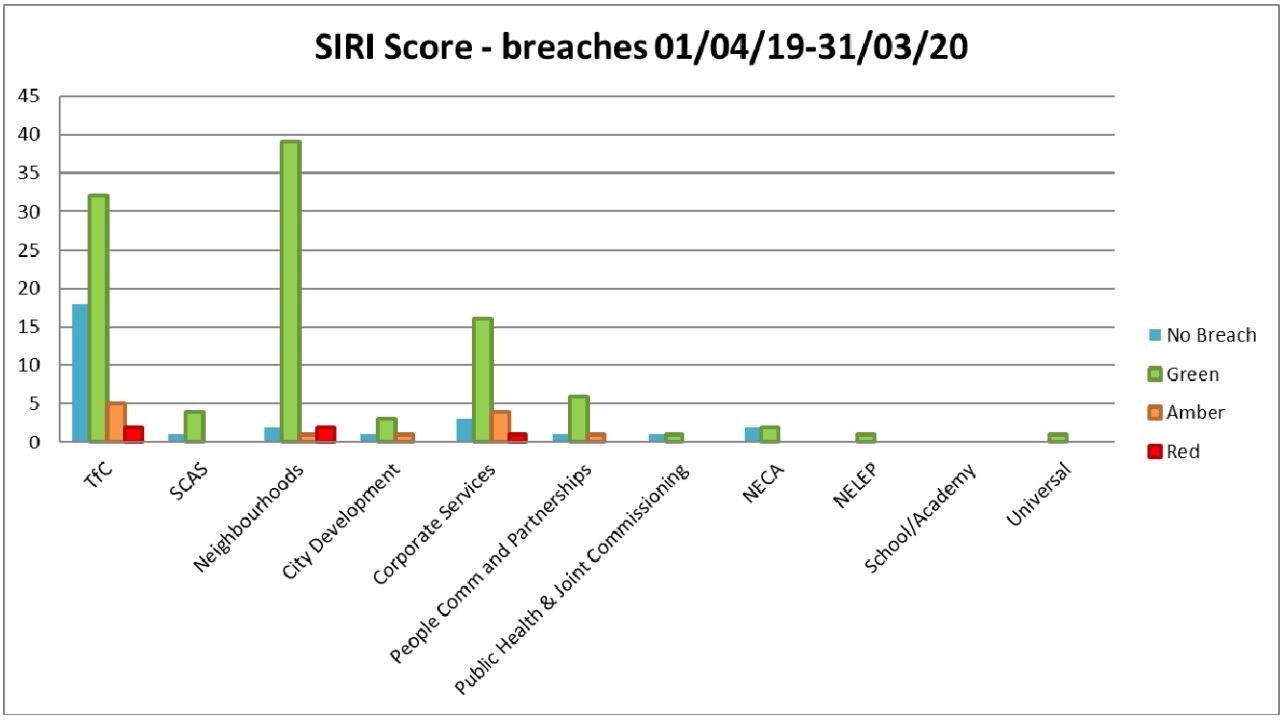
13. REPORT CONTACT

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

APPENDIX A

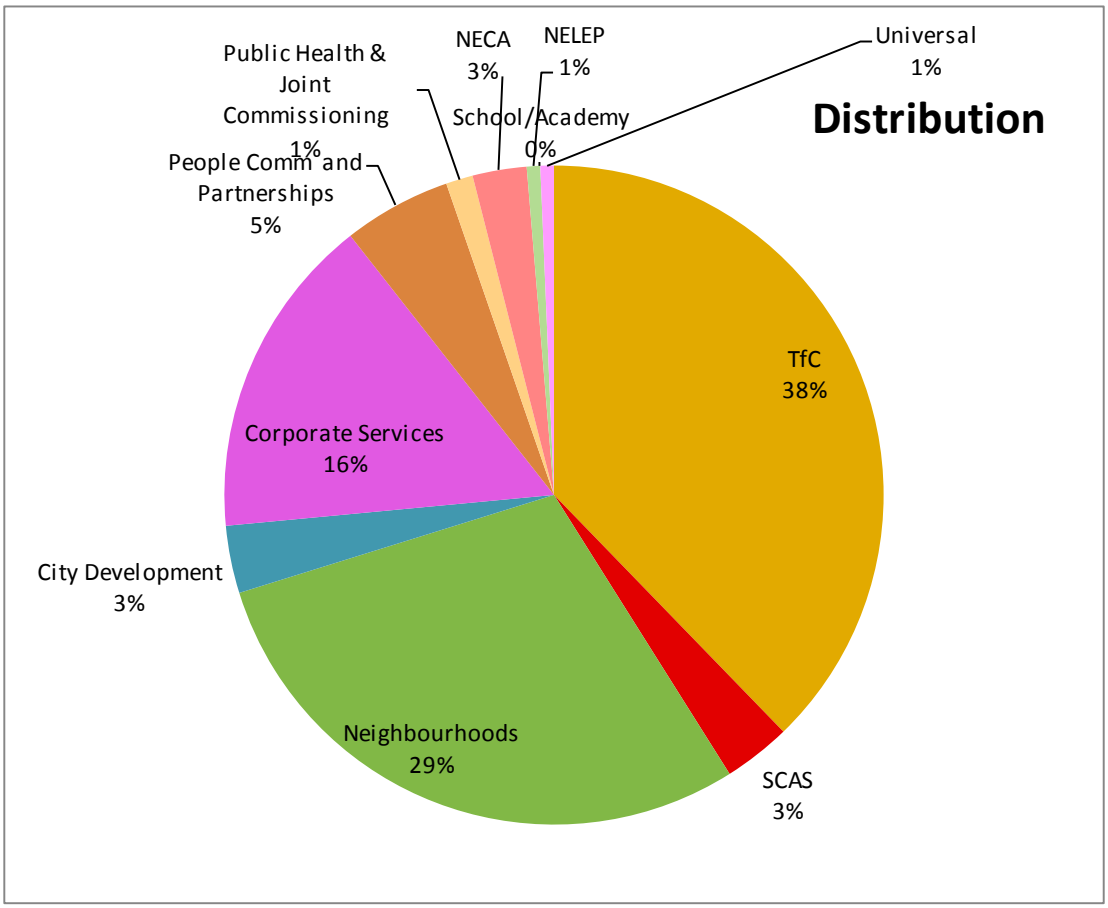
Number reported 2018-19	Compliance issues	Measure Description	Number at 1 April 2019 - 31 March 2020
7	ICO Reported	Number of personal data breaches reported to the Information Commissioners Office (ICO)	5 (4x Council Reports, 1x supplier report)
4	ICO report Civic	Number of breaches self-reported to the Information Commissioners Officer (ICO)	5
3	ICO report Public	Number of customer reports to the Information Commissioners Officer (ICO) by a member of the public alleging a personal data breach.	0
170	Breach Total	The total number of cases where a report or request for advice has identified a failing in Data Protection compliance	122
4	Red	Number of cases where a personal data breach via SIRI - Serious Incidents Requiring Investigation - Red Rating	5
50	Amber	Number of cases where a personal data breach has been reported or identified via SIRI - Serious Incidents Requiring Investigation - Amber Rating	12
105	Green	Number of cases where a personal data breach has been identified via SIRI - Serious Incidents Requiring Investigation - Green Rating	105
11	Compliance Issue (non-breach)	Data Protection Compliance issue (non-article 4)	29

APPENDIX A

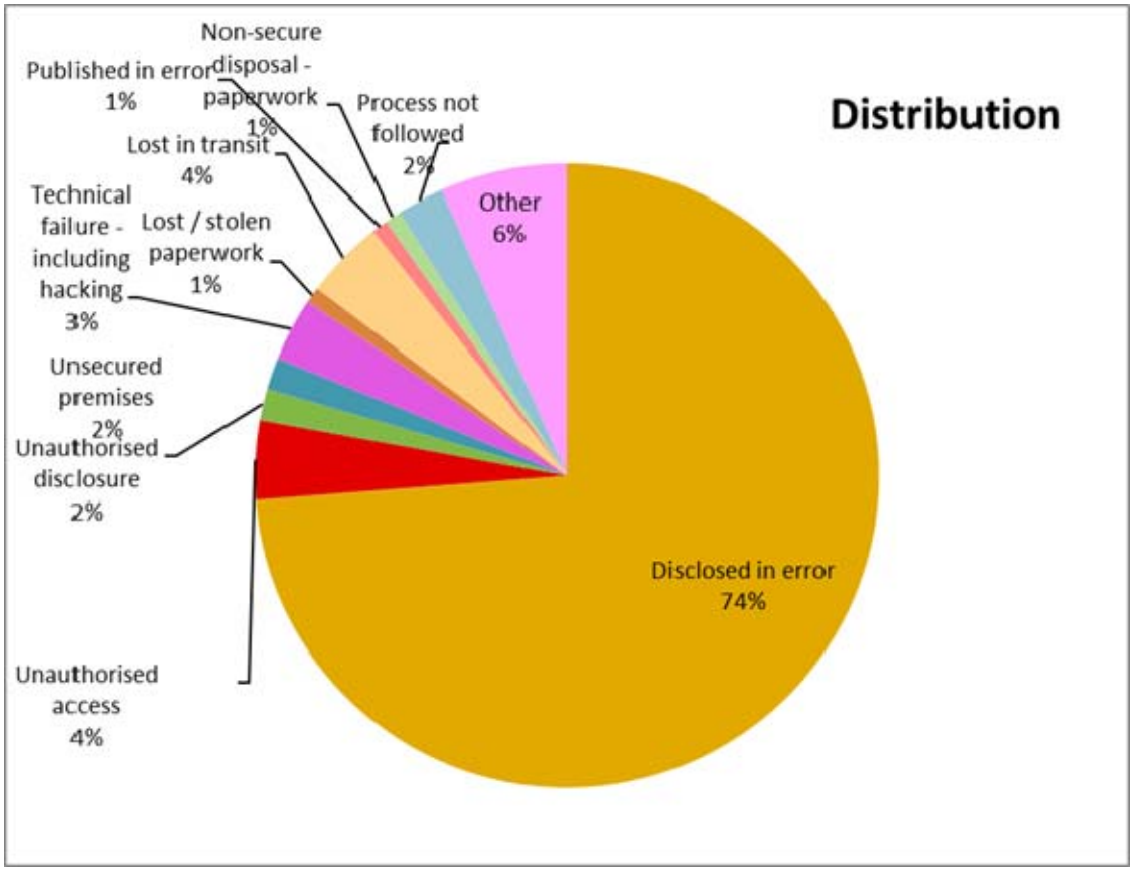


breach recording data 1/4/19-31/3/20	TfC	SCAS	Neighbourhoods	City Development	Corporate Services	People Comm and Partnerships	Public Health & Joint Commissioning	NECA	NELEP	School/Academy	Universal	Total
Green	32	4	39	3	16	6	1	2	1	0	1	105
Amber	5	0	1	1	4	1	0	0	0	0	0	12
Red	2	0	2	0	1	0	0	0	0	0	0	5
No Breach	18	1	2	1	3	1	1	2	0	0	0	29
Total (srvs)	57	5	44	5	24	8	2	4	1	0	1	151

APPENDIX B


Distribution
Universal 1%
NELEP 1%
NECA 3%
Public Health & Joint Commissioning 1%
School/Academy 0%
People Comm and Partnerships 5%
TfC 38%
Corporate Services 16%
City Development 3%
Neighbourhoods 29%
SCAS 3%

APPENDIX B


Distribution
Non-secure disposal - paperwork 1%
Published in error 1%
Process not followed 2%
Lost in transit 4%
Other 6%
Technical failure - including hacking 3%
Lost / stolen paperwork 1%
Unsecured premises 2%
Unauthorised disclosure 2%
Disclosed in error 74%
Unauthorised access 4%

breach recording data 1/4/19-31/3/20	Apr-19	May-19	Jun-19	Jul-19	Aug-19	Sep-19	Oct-19	Nov-19	Dec-19	Jan-20	Feb-20	Mar-20	Total	Average per Month
Disclosed in error	9	14	7	11	2	3	6	4	4	7	13	10	90	7.5
Unauthorised access					1	1			1	1	1		5	0.4
Unauthorised disclosure								1	1				2	0.2
Unsecured premises		1					1						2	0.2
Technical failure - including hacking	1				1				1		1		4	0.3
Lost / stolen paperwork			1										1	0.1
Lost in transit			1	1		1					2		5	0.4
Published in error				1									1	0.1
Non-secure disposal - paperwork			1										1	0.1
Process not followed						1			1	1			3	0.3
Other				2	1		1	1	1	1	1		8	0.7
Total (srvs)	10	15	10	15	5	6	8	6	9	10	18	10	122	10.2