Committee: Digital Services Sub (Finance) Committee	**Dated:** 03.09.2021
Subject: Data Protection - 2020 Annual Report	**Public**
Report of: Michael Cogher Comptroller & City Solicitor	**For Information**
Report author: Sophie Jordan Compliance Manager – DP & FOI	

Summary

A high standard of compliance with the legislation was maintained in 2020 at a corporate and departmental level, in the context of challenges presented by the Covid-19 pandemic, and the subsequent changes to existing Data Protection legislation as a result of wider Brexit implications.

Recommendation(s)

Members are requested to note the report.

Main Report

Background

1. This is the eighth annual report in respect of corporate and departmental compliance with the Data Protection Act 2018.

2. The Data Protection Act 2018 (DPA 2018) governs everything the City of London (CoL) does with personal information (which is any information relating to an identifiable, living person), from collection/creation to destruction, in any medium. It applies to the whole of the CoL. However, the following are data controllers in their own right: City of London Police; Sir John Cass's Foundation Primary School; Museum of London; Members as to their Ward work; and the Electoral Registration Officer.

3. In addition to the DPA 2018, the CoL also processes personal data in accordance with the European Union General Data Protection Regulation (EU GDPR), as established on the 25 May 2018. It is noted that following Brexit agreements, there will be a new version of the GDPR implemented, known as the United Kingdom General Data Protection Regulation (UK GDPR), which will also apply to the personal data processed by the CoL.

4. The risk of Data Protection breaches, given that the CoL routinely processes personal information, is overseen as part of Corporate Risk 16, Information Governance, and Corporate Risk 25, GDPR Project.

5. Co-ordination of the DP compliance work is undertaken by the Compliance Team who are based, in the Comptroller & City Solicitor's Department,

6. The Comptroller & City Solicitor, to whom the Compliance Team reports in respect of data protection matters, is the CoL's designated Data Protection Officer (DPO). A designation is required under Article 37 of the EU and UK GDPR.

7. Each department has a responsibility for the personal information it holds and a shared responsibility for compliance with the DP requirements. To assist with departmental responsibility and corporate coordination, the Information Officer (as was) established, in 2003, an Access to Information Network (AIN), with one or more representatives in every Department. The duties of an AIN were formalised in a memo in 2003[1] and consist, in summary of assisting in ensuring all aspects of compliance within their areas with the FOI, EIR, Data Protection Act 2018 (DPA) and Re-use of Public Sector information (RePSI) legislations.

Breaches or Potential Breaches

8. The Information Commissioner can fine data controllers up to £17million for breaches of the DPA 2018, and/or impose enforcement action such as an Enforcement Notice (to not comply with which would be a criminal offence), or an Undertaking, which is a more informal approach but still potentially onerous. To date it is noted that the CoL has never received any fines or other enforcement action.

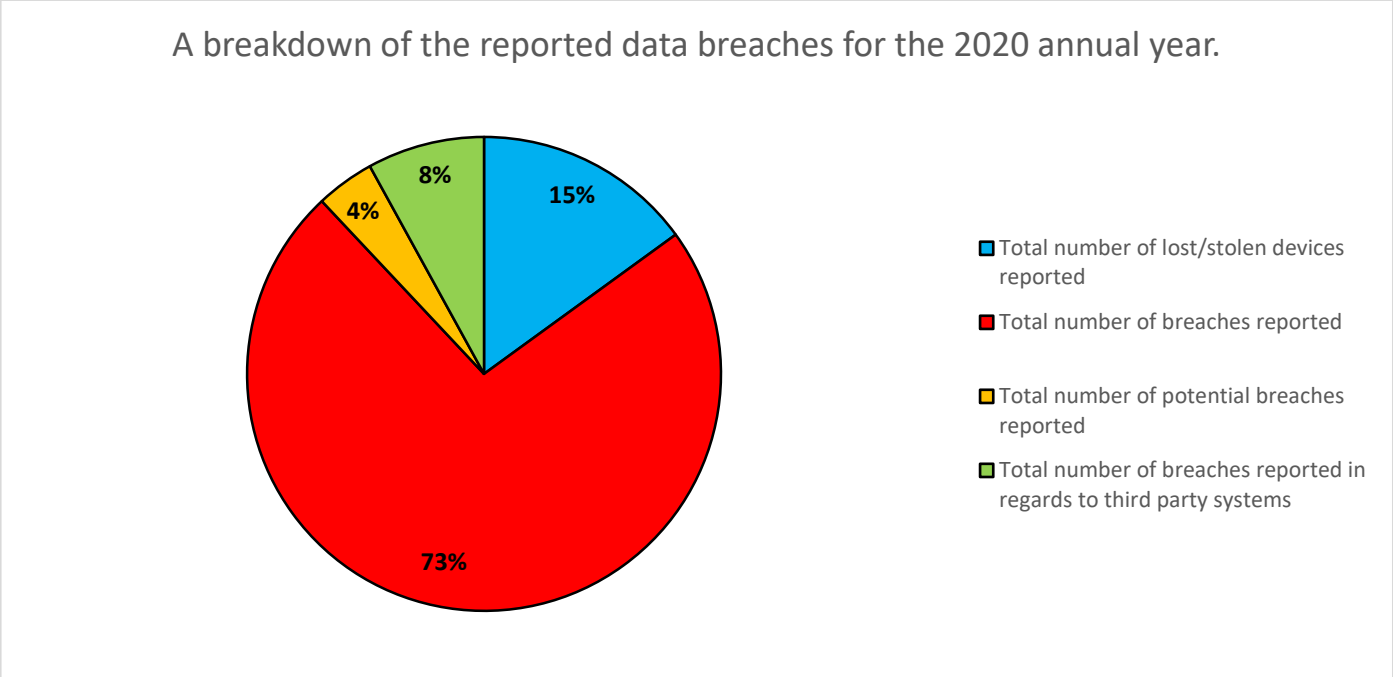
9. All breaches, or potential breaches[2], of the DPA 2018 are required to be reported to the Compliance Team and the relevant departmental AIN Representative, as soon as known, and subsequently to the DPO and members if the breach is deemed to present a high level of risk. To ensure we meet legal requirements as to any required reporting by the DPO to the regulator (the Information Commissioner), all breaches should be reported to the Compliance Team and AIN Representative within 72 hours of the staff member becoming aware of the incident, irrespective of the level of risk. To assist this process there is a DP Breach Notification Form held on the CoL's Intranet, and available on request from the Compliance Team.

10. The Compliance Team assists the Department in managing the breach or potential breach. This may include assisting with formal apologies, contacting unintended recipients of information, reinforcing training requirements, and ensuring that staff understand the procedures to be followed to prevent a recurrence. Should a breach be considered as presenting a significant level of risk then an investigation report is produced for the Data Protection Officer.

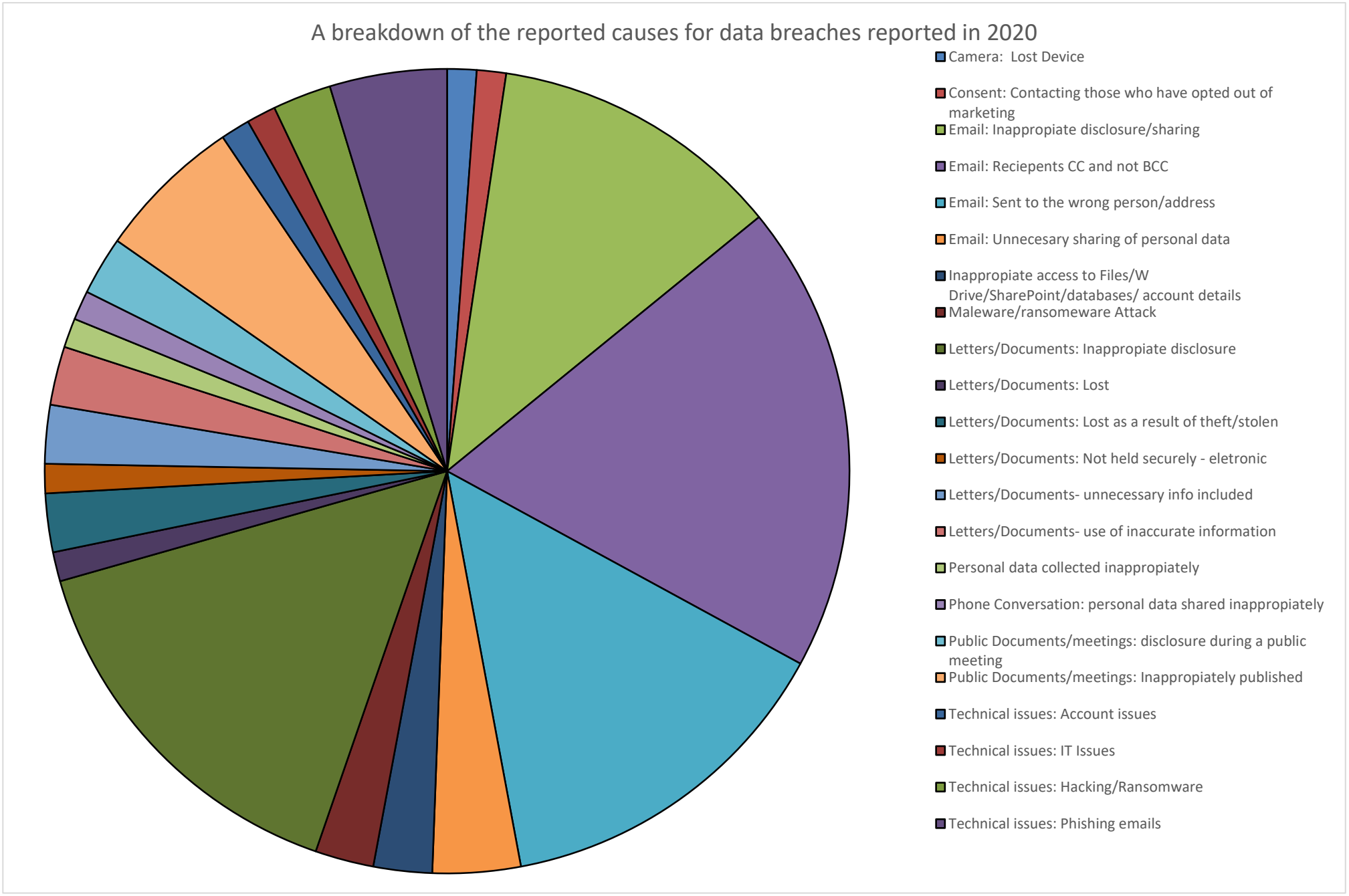
11. In the 2020 annual year there were 100 reported breaches. Of these,15 were in regard to devices that were reported as lost/stolen, but all devices had been encrypted and disabled, or otherwise protected and so no breach or potential breach was raised. Nevertheless, as in previous years, they are included in the total annual figure (please see paragraph 17 for annual totals). Of the remainder, 73 breaches and 4 potential breaches and 8 breaches that were the fault of a third-party provider were recorded under the DPA 2018.

[1] Memo for AIN role 2003

[2] 'Potential breaches' are where breaches are not proven even though the circumstances may suggest that a breach has occurred.

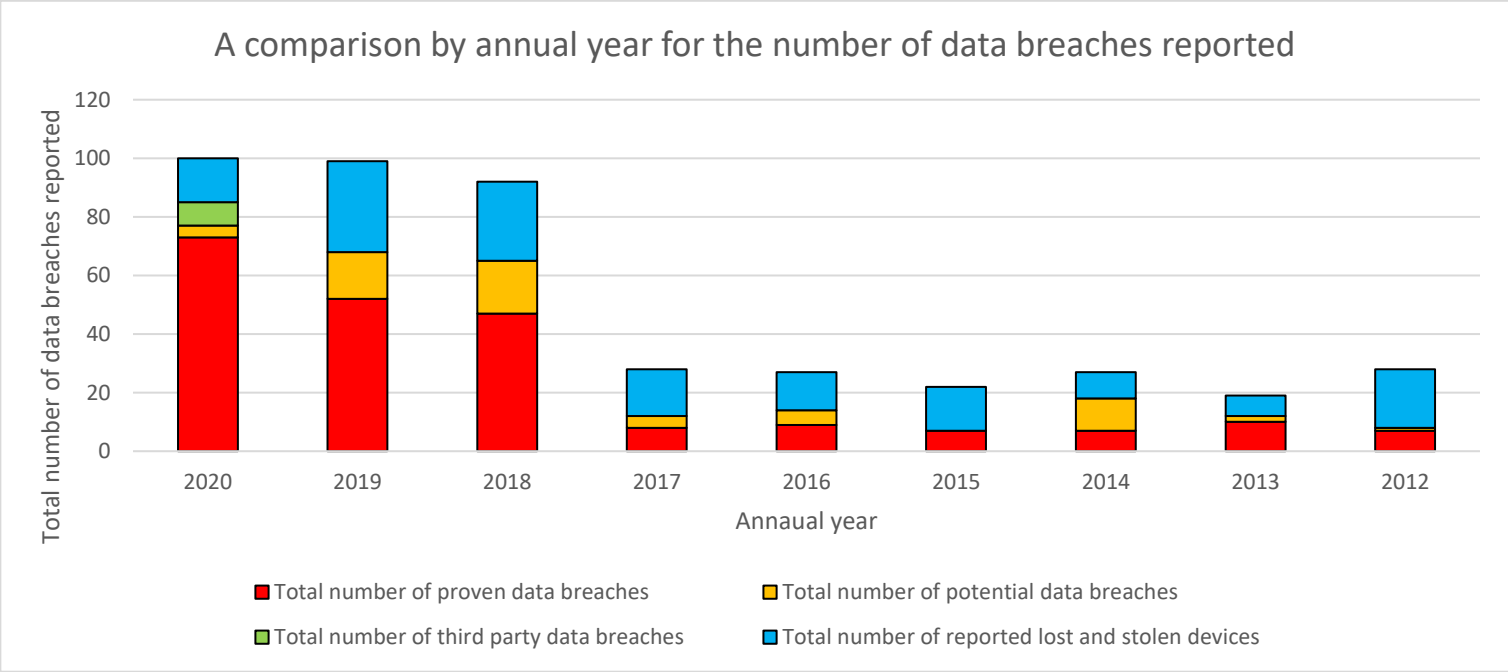


12. During the 2020 annual year there were 85 instances of either a data breach, potential data breach or a data breach relating to a third party reported. Please see the following pie chart for a breakdown of causes for these breaches.


A breakdown of the reported causes for data breaches reported in 2020
Camera: Lost Device
Consent: Contacting those who have opted out of marketing
Email: Inappropiate disclosure/sharing
Email: Reciepents CC and not BCC
Email: Sent to the wrong person/address
Email: Unnecesary sharing of personal data
Inappropiate access to Files/W Drive/SharePoint/databases/ account details
Maleware/ransomeware Attack
Letters/Documents: Inappropiate disclosure
Letters/Documents: Lost
Letters/Documents: Lost as a result of theft/stolen
Letters/Documents: Not held securely - eletronic
Letters/Documents- unnecessary info included
Letters/Documents- use of inaccurate information
Personal data collected inappropiately
Phone Conversation: personal data shared inappropiately
Public Documents/meetings: disclosure during a public meeting
Public Documents/meetings: Inappropiately published
Technical issues: Account issues
Technical issues: IT Issues
Technical issues: Hacking/Ransomware
Technical issues: Phishing emails

13. Of the 85 breaches reported, 73 were found to be proven breaches. Of the 73 proven breaches only 1 was considered to demonstrate a high level of risk, thereby meeting the criteria necessary for reporting the incident to Information Commissioner Office. It is noted that in this case the Commissioner did not issue enforcement action.

14. Figures for breaches reported to the Compliance Team are as follows, please see **appendix one** for a further breakdown:



*Please note that prior to 2020, third party data breaches were included in the totals reported for proven data breaches.

15. The increase in reported breaches in 2020 is considered an outcome of greatly increased vigilance by departments in the context of the much stricter requirements of the DPA 2018, including reporting requirements, coupled with greater staff awareness of DP issues as a result of both internal communications, campaigns and external media reporting. It is also evident that while the numbers have increased, the severity of the cases has not.

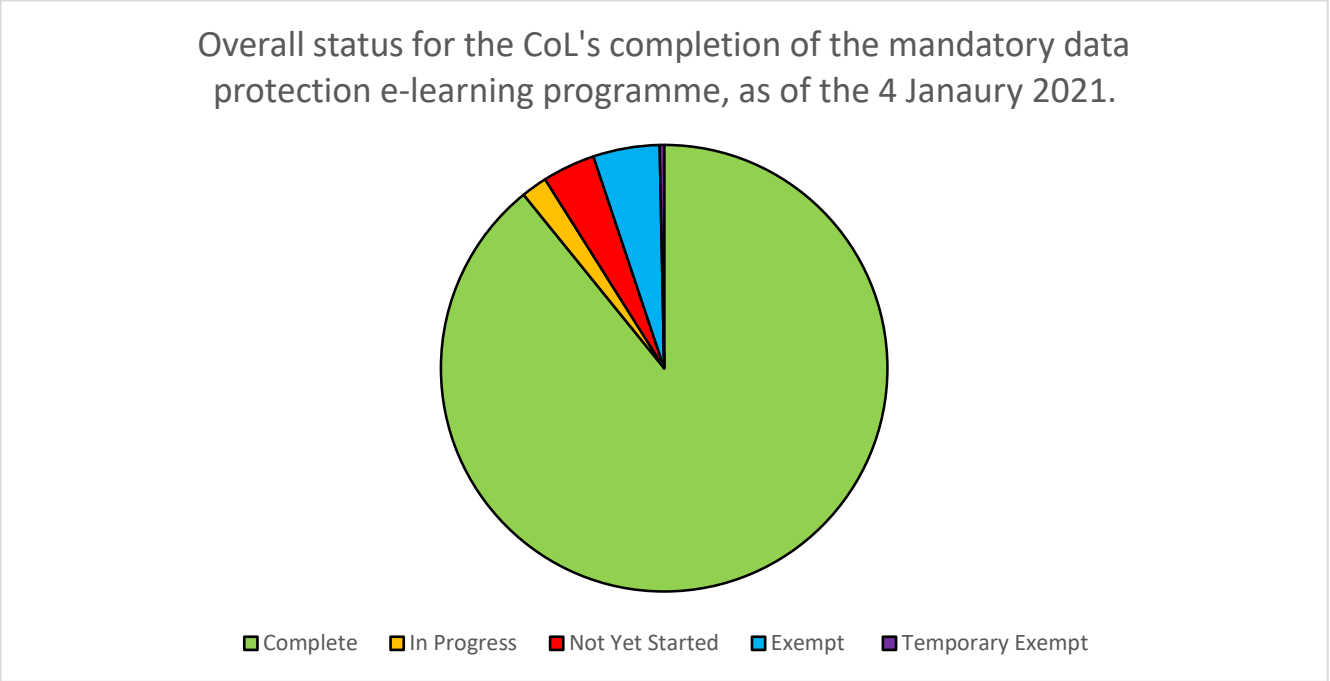
DP Guidance

16. The Compliance Team routinely provides departments, on request, with DP guidance on specific issues. In addition, there has been since 2004 considerable DP guidance for staff on the Access to Information Intranet pages, provided by the Compliance Team and is in the process of being updated, as required, in line with the new legislation. In addition, a Microsoft Teams site has also been established in order to provide quick guidance to AIN reps.

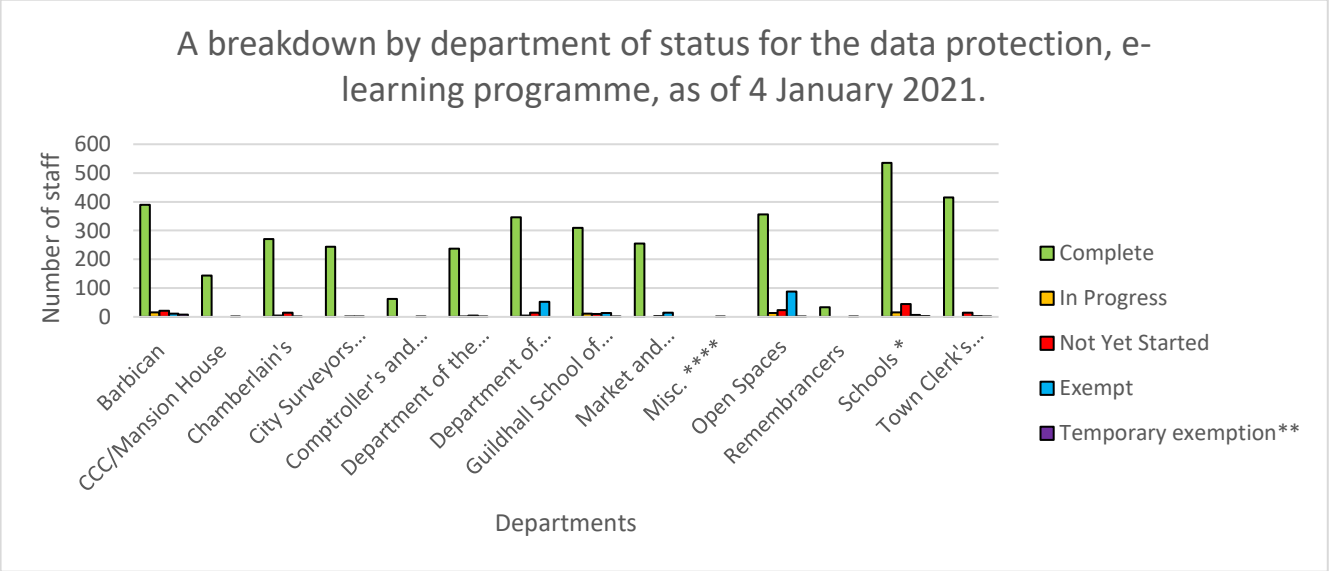
DP Training

17. There has been a high uptake of the new e-learning mandatory data protection package. At the end of the 2020 annual year the overall figure for the City of London

was that 94.30% of staff had completed training (this figure includes a small percentage that were made exempt or temporally exempt).



The Compliance team continues to review and monitor the uptake of the data protection training and provides reports to Chief Officers on an annual basis. A breakdown by of completion status by department is provided below, with further information provided in **appendix 2.**



DP Auditing

18. The annual CoL DP audit did not take place in 2020 due to the impact of Covid-19 on working practices. The annual DP audit requires a review of physical working environments and therefore has been put on hold until the majority of staff are able to return to the office environment.

19. An external audit undertaken by Mazars in July 2019 with regards to the implementation of GDPR, which found that the CoL had achieved moderate assurance with the GDPR (having an adequate control framework in place but weaknesses…

which may put some system objectives at risk) and that the CoL was in the progress of becoming fully compliant. Internal Audit undertook a further review of the key areas highlighted by the Mazars report.

- Continued monitoring of the mandatory Data Protection training.
- A review of the corporate 'W' drive.
- A review of the retention policies
- The re-introduction of the annual DP audit.

20. Following the further review by internal audit, it was found that the following areas highlighted by Mazars were no longer valid:

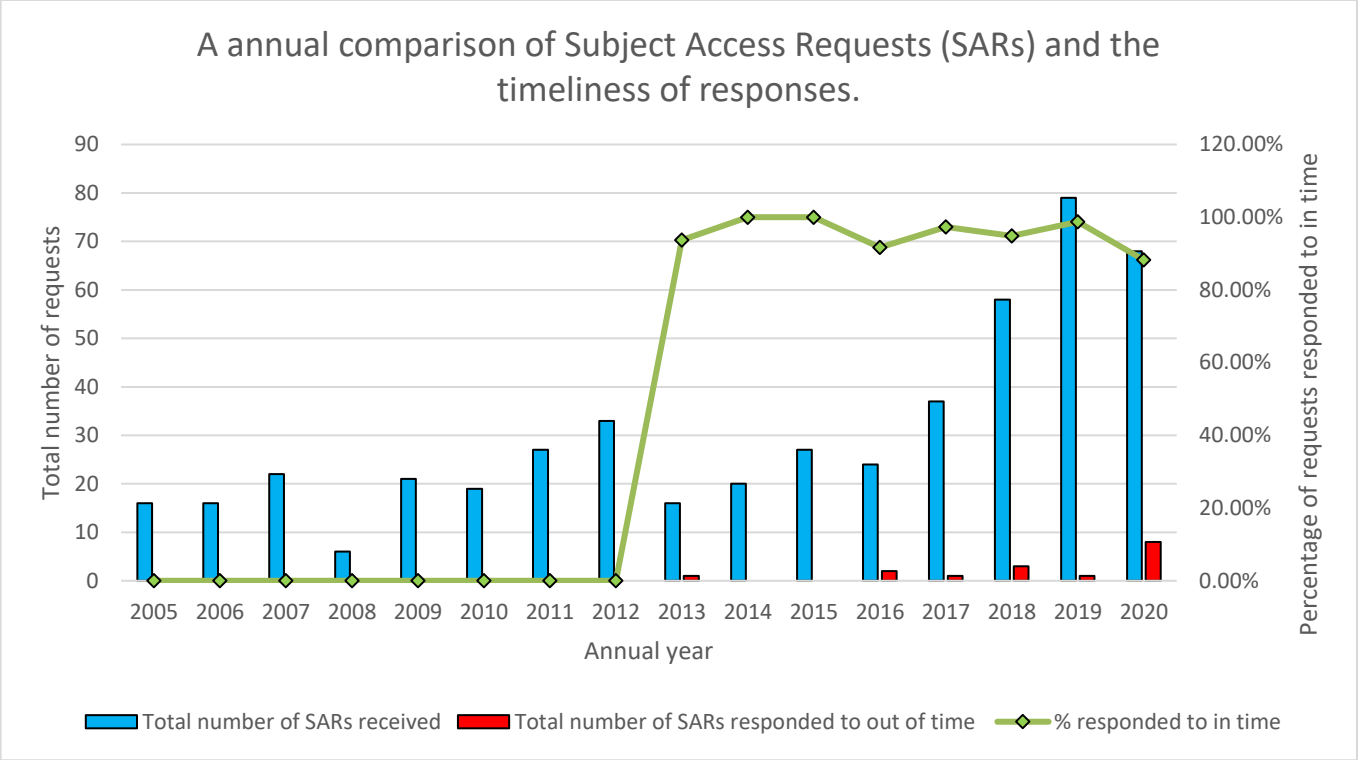
    - Continued monitoring of the mandatory Data Protection training.
    - The re-introduction of the annual DP audit.

    However, the remaining two areas highlighted by Mazars required continued review and were implemented with revised action dates of 31 December 2021.
    - A review of the corporate 'W' drive.
    - A review of the retention policies

    These considerations were reviewed and have been incorporated into the relevant departments ongoing work.

Subject Access Requests

21. Subject Access Requests (SARs) made under the DP legislation are where the subjects of personal information ('data subjects') exercise their right to make requests to be provided with copies of the personal information held about them by a data controller. A data controller has, under the DPA 2018, a calendar month, in which to comply, ie to disclose or apply relevant exemptions or other constraints under the legislation. The CoL received 69 SARs in 2020, under the DPA 2018. Of these, 60 were complied with within the statutory timescale, a compliance rate of 86.95%. A further breakdown can be found at **Appendix three.**



*Please note that no data is held for requests prior to 2013.

22. The 2020 compliance rate has decreased since 2019 from 98.73% to 88.24%. However, it is noted that compliance with SARs were impacted by the wider effects of the Covid-19 pandemic, with departments experiencing increased workloads and additional duties in addition to paper documents being inaccessible as a result of staff working from home during the national lockdowns.

23. Data subjects are also exercising other rights under the new legislation, which rights, while not being greatly different in substance compared with the DPA 1998, have been more publicised as a result of the introduction of the new legislation and considerably more exercised. The updated rights (all subject to caveats and exemptions) are: the right to rectification of purportedly inaccurate personal data; the right to erasure (also known as the 'right to be forgotten'); the right to restriction of processing; right to be informed as to what of their data is being processed; right to data portability, where the data subjects can request that the personal data held on them is transferred to a different company/organisation; the right to object to processing; and the right to object to automated processing, where, should a decision be made without human interaction, the data subject can request that the decision is reviewed by a human.

24. In 2020, under the DPA 2018, the CoL received 79 requests for erasure, 1 request for data portability and 3 requests for rectification (there were no other requests made for any other rights applicable under the DPA 2018). Of these 80 were completed in accordance with the statutory timescale (1 month), a compliance rate of 96.38%.

25. The 2020 total is the highest number of requests made in regard to other data subject rights, in a year since records were first kept in 2018 and is considered to be the result of an increased awareness by data subjects of their rights.

Complaints

26. There were 13 complaints received:

- 5 regarding personal data processed as part of the new swimming season tickets for the Hampstead Heath Swimming Ponds (5 partially upheld)
- 3 regarding the use and sharing of personal data (1 not upheld, 1 partially upheld, 1under investigation)
- 2 regarding the response provided to a SAR (1 not upheld-no response received to clarification request, 1 partially upheld)
- 1 regarding a request for personal data to be provided as proof of identification (not upheld)
- 1 regarding the allegation of a data breach (not upheld)
- 1 concerning the use of Zoom to record lessons (not upheld)

Notifications

27. In accordance with DP legislation, data controllers are required to notify with the ICO. Under the DPA 2018, the process had been streamlined, in that a detailed description of processing is no longer required. Instead, data controllers register using the set form for the relevant class of data controller into which they fall. A more detailed description is, though, required to be kept by each data controller (please see 'Record of Processing Activities (RoPA)', below). All notifications must be kept up to date and renewed annually with the ICO, for which the ICO levies a charge. The Compliance Team are responsible for maintaining the CoL's notification and that of the Electoral Registration Officer.

GDPR

28. **General**: In practice, while the DPA 2018 and GDPR requirements represented a wholesale revision of DP law, it is more a case of degree than kind, putting best practice into law. There is also a reasonableness element in the GDPR, a recognition that compliance can take into account the costs involved, measured against risks. We should not be complacent. As ever, it is important that the CoL takes a corporate, structured approach to compliance which is robust. As mentioned in previous reports, the administrative fines for non-compliance under the GDPR are "up to £17 million, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher"[3]. For the purpose of administrative fines, "an undertaking should be understood to be an undertaking in accordance with Articles 101 and 102 TFEU"[4].

29. During 2020, in accordance with the ongoing Brexit negotiations the Compliance Team continued to monitor and provided advice in regards to the EU GDPR while helping departments to prepare for any changes brought about by the Brexit agreement, This included reviewing the geographical location for where personal data is held and then updating any agreements or arrangements that are in place. For example advising that the data is held on a server/cloud based within the United Kingdom, or requesting that departments implement the EU Standard Contractual Clauses for data protection, in all contracts and agreements, as opposed to relying on previous lawful basis i.e. an adequacy decision.

[3] Article 83 of the GDPR
[4] Recital 150 of the GDPR.

30. We note that as of the 1 January 2021, the UK government and EU commission had not agreed on a formal adequacy decision to allow for the transfer of personal data between the UK and EEA countries. As such we continued to monitor the situation as it developed.

    It is noted that a formal adequacy decision between the UK and EEA countries was agreed on the 28 June 2021, allowing the transfer of personal data between the UK and the relevant EEA country without any further actions being required. However, it is noted that the formal adequacy decision has been agreed for a period of 4 years, with the view to the agreement potentially being renewed after that time. Also, it should be noted that the adequacy decision can be revoked at any time prior to the 4 years expiring.

31. **Data Protection Officer (DPO)**: As mentioned, Article 37 of the GDPR requires a data controller to have a designated DPO and the Comptroller & City Solicitor is that Officer for the CoL and is also the DPO for the Town Clerk in his role as Electoral Registration Officer, the Town Clerk being a separate data controller from the CoL in that capacity.

32. **Policies and Corporate Privacy Notices**: Following the changes brought about by the EU GDPR, the Compliance team, alongside colleagues within the Comptrollers and AIN reps have continued to review, maintain and where necessary update all the privacy notices and policies in respect of the new and updated activities that the CoL have been undertaking which involved personal data. The Responsibility for these belongs with the Compliance Team and the respective departments.

33. **Record of Processing Activities (RoPA)**: This is the core document in providing an audit of personal data processing, in accordance with Article 30 of the GDPR. The master version created and maintained by the Compliance Team continues to collect additional processing information the recording of which is required under other Articles of the GDPR, with the aim of creating a single, updateable record of the CoL's processing. The RoPA project continues to be managed via the AIN, with the Compliance Team overseeing and providing guidance where required. This is a living document that requires regular updates and review. The Compliance Team hold and update a master version, that we hope to make accessible to all staff.

Conclusion

34. The processing of personal information is a continuous activity across most of our functions and so we always live with the possibility of ordinary human error. Nevertheless, guidance, training and awareness raising contribute effectively to the CoL's compliance with the DPA 2018. Just one mistake can have considerable implications. Nevertheless, while we should not lower our guard, it can be said that all departments appeared in 2020 to be achieving a good level of compliance with the new legislation.

35. The AIN and other staff across the CoL have reacted very positively to the implementation of GDPR and work hard to ensure that the CoL is compliant with the DPA 2018 and remains so, including in relation to any new processing activities, with enquiries being made to the Compliance Team and Legal staff in the Comptroller & City Solicitor's Department on a daily basis.

Appendices:
Appendix1: CoL – A breakdown of data breaches reported by annual year.
Appendix 2: CoL- A breakdown of statistics for the data protection e-learning programme.
Appendix 3: CoL- A breakdown of statistics for the timeliness of responding to SARs.

Michael Cogher
Comptroller and City Solicitor
T: 020 7332 3699
E: michael.cogher@cityoflondon.gov.uk

Appendix 1: CoL- A breakdown of data breaches reported by annual year

Year	Total breaches reported	Proven	Non-proven (Including lost and stolen devices)	Proven Breaches as a result of a third party
2020	100	73	19	8
2019	99	52	47	Data not recorded
2018	92	47	45	Data not recorded
2017	28	8	20	Data not recorded
2016	27	9	18	Data not recorded
2015	21	7	14	Data not recorded
2014	27	7	20	Data not recorded
2013	19	10	9	Data not recorded
2012	28	7	21	Data not recorded

Appendix two: CoL statistics for the completion of the Data Protection e-learning programme.

CoL status	Total	Percentage
Complete	3595	89.16%
In Progress	76	1.88%
Not Yet Started	154	3.82%
Exempt	194	4.81%
Temporary Exempt	13	0.32%
Total	**4032**	**100.00%**

Please note that for the following table:

* Please note schools is a combined total, for a further breakdown please see the tab below.

** Those marked temporary exempt will need to complete the training on their return to work

*** The percentage for the overall completion is a combined percentage of those who have completed; been made exempt or marked as temporary exempt.

**** These members of staff are either temporary or contractors, who have not been assigned a department

Department	Complete	Percentage	In Progress	Percentage	Not Yet Started	Percentage	Exempt	Percentage	Temporary exemption**	Percentage	Totals	Overall completion***
Barbican	389	87.42%	16	3.60%	21	4.72%	11	2.47%	8	1.80%	445	91.69%
CCC/Mansion House	144	99.31%	0	0.00%	0	0.00%	1	0.69%	0	0.00%	145	100.00%
Chamberlain's	270	92.78%	5	1.72%	15	5.15%	1	0.34%	0	0.00%	291	93.13%
City Surveyors Department	244	99.19%	0	0.00%	1	0.41%	1	0.41%	0	0.00%	246	99.59%
Comptroller's and City Solicitors	62	98.41%	0	0.00%	0	0.00%	1	1.59%	0	0.00%	63	100.00%
Department of the Built Environment	237	97.13%	1	0.41%	5	2.05%	1	0.41%	0	0.00%	244	97.54%
Department of Communities and Children's Services	346	82.97%	4	0.96%	15	3.60%	52	12.47%	0	0.00%	417	95.44%
Guildhall School of Music and Drama	309	89.83%	11	3.20%	10	2.91%	13	3.78%	1	0.29%	344	93.90%
Market and Consumer Protection	255	93.75%	0	0.00%	2	0.74%	15	5.51%	0	0.00%	272	99.26%
Misc. ****	0	0.00%	0	0.00%	1	100.00%	0	0.00%	0	0.00%	1	0.00%
Open Spaces	356	73.86%	13	2.70%	24	4.98%	88	18.26%	1	0.21%	482	92.32%
Remembrancers	33	97.06%	0	0.00%	0	0.00%	1	2.94%	0	0.00%	34	100.00%
Schools *	535	88.43%	16	2.64%	45	7.44%	7	1.16%	2	0.33%	605	89.92%
Town Clerk's Department	415	93.68%	10	2.26%	15	3.39%	2	0.45%	1	0.23%	443	94.36%
	3595		76		154		194		13		4032	

Appendix 3: CoL- A breakdown of statistics for the timeliness of responding to SARs.

Annual Year	Total number of SARs received	Total number of SARs respond to in time	Total number of SARs responded out of time	Percentage of SARs responded to in time
2005	16			0.00%
2006	16			0.00%
2007	22			0.00%
2008	6			0.00%
2009	21			0.00%
2010	19			0.00%
2011	27			0.00%
2012	33			0.00%
2013	16	15	1	93.75%
2014	20	20	0	100.00%
2015	27	27	0	100.00%
2016	24	22	2	91.67%
2017	37	36	1	97.30%
2018	58	55	3	94.83%
2019	79	78	1	98.73%
2020	68	60	8	88.24%

- Please note that no data is held prior to 2013.