CYNGOR SIR *POWYS* COUNTY COUNCIL.

CABINET EXECUTIVE
9th July 2019

REPORT AUTHOR:	**County Councillor James Evans** **Portfolio Holder for Corporate Governance, Housing and Public Protection**
SUBJECT:	**Annual Information Governance (IG) report 2018-2019**
REPORT FOR:	**Information**

1. Background

1.1 Powys County Council has in place an Information Management Assurance Governance (IMAG) plan to initiate, develop, and monitor policies and practices in relation to information security, information management, and information risk, to ensure compliance with relevant information legislation and standards.

1.2 In addition a separate General Data Protection Regulation (GDPR) plan was utilised to prepare for the implementation of new legislation and to identify and manage preparatory activity.

1.3 This report is to brief the Senior Information Risk Owner (SIRO) and the Corporate Information Governance Group (CIGG) on the IG practices implemented and the standards of IG compliance achieved for the financial year 2018/19.

1.4 The report is supported by the following appendices

- Appendix 1 – ICO Enforcement Training
- Appendix 2 – Information security incident breakdown
- Appendix 3 - Information requests due each quarter by service area
- Appendix 4 - Information Compliance team structure.

2. Proposal

2.1 For Cabinet to note the content of the annual IG report

3. Information Management Assurance and Governance (IMAG) Plan

3.1 The current IMAG plan was agreed in March 2017, to cover 2017 – 2019, and included high level actions required for compliance with GDPR upon its implementation in May 2018.

3.2 Regular quarterly CIGG meetings have taken place through the year where the activity undertaken has been considered, and challenged,

where timescales were not met. The March 2018 meeting concentrated solely on GDPR preparation.

3.3 Early in the financial year the majority of work being undertaken was for the preparation of GDPR, which included policy revision, and Information Asset Audit work, resulting in Powys County Council putting in place Information Asset Registers, for the first time. The registers record the information held by the Council, the purpose, location and owners. Going forward these will provide the base for records of processing activities and information audits.

3.4 The Senior Information Risk Owner changed in April 2018 from the Strategic Director for Place to the Director for Resources, and again in February 2019 to the Head of Legal and Democratic Services, due to the departure of the previous post holders and a restructure of senior positions within Powys County Council.

3.5 A revised IMAG plan for 2019 – 2021 was agreed by CIGG in March 2019.

3.6 Additionally regular Corporate Information Governance Operational Group (CIOG) meetings have taken place, with revitalised membership, involving representatives of the Information Asset Owners, to discuss and monitor IG matters and measurements and to carry out the work activities as directed by the CIGG.

4. ICO Enforcement Training

4.1 In line with the ICO's enforcement order against Powys County Council in December 2012, staff with access to personal data undertake training in the basics of the Data Protection and also the organisation's information policies.

4.2 Monthly reports have been provided for Heads of Service to identify their staff who are non-compliant in order to take necessary action, ensuring compliance for their service area.

4.3 As at 2nd April 2019,

- The number of staff with access to personal data is 2,188
- The number of staff trained is 1,889
- Powys County Council's compliance rate is 86.33%, with a self-imposed target of 98%.

4.4 In April 2018 the compliance rate was 84.18%.

4.4.1 (For departmental breakdown see Appendix 1)

4.5 Current courses are to be replaced with Cyber Security and GDPR, which still meet the ICO enforcement order, but includes information on cyber security issues. Due to the speed at which cyber security issues

change and develop then the decision was made to change the refresh period to an annual refresh. This also meets the recommendations of the regulator.

4.6 The training compliance figures form part of the IG measurements provided to CIGG.

5. **Information Security Incidents**

5.1 Even prior to the changes of personal data breach notification to the ICO contained within the GDPR, the council had robust information personal data breach reporting and management processes in place, which continues to ensure swift containment action, informed identification of information risks and mitigation, and supports the regulatory reporting requirements.

5.2 The table below provides details of incidents and personal data breaches, and comparison data from last year.

	2017/2018	2018/2019
Numbers of reported incidents	127	176
Number of breaches of the Data Protection Act	13	71 *
Number of incidents reported to the ICO	3	25
Number of notifications to data subjects	NA	11
Number of complaints made to the ICO over personal data breaches	3	3
Number of DPA breaches occurring externally	12	52
Number of DPA breaches occurring internally	1	17
Number of DPA breaches involving sensitive personal data	5	22
Number of DPA breaches contained	10	56

* using the definition of a personal data breach within GDPR. A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a public electronic communications service

5.3 Increased reporting of information security incidents and personal data breaches can be attributed to awareness being raised of GDPR, changes to what is constitutes a breach, and the new notification requirements and from media stories in relation to the amount of the new monetary penalties able to be used by the regulator.

5.4 Personal data breaches notified to the ICO include, misdirection of staff disciplinary information, disclosure of email addresses, disclosure of information to the press, misdirection of information through email or postal processes.

5.5 One outcome of such complaints, has been for Development Management to take the decision to no longer publish public representations to planning applications, on the council's web pages.

5.6 The ICO has chosen not to take any regulatory action in these cases, but has made a number of recommendations. Such as annual staff training, relevant information being provided to data subjects, revision of policies, reviewing processes, revision of staff contracts, use of delivery methods, and use of peer checking.

5.7 There has been an increase of individuals taking their complaints directly to the ICO. Those made related to disclosure without consent and disclosure of email addresses through planning process.

5.8 In all 3 cases of complaint the ICO found that the Council had breached data protection legislation, to varying extents.

5.9 The reporting and management of information security incidents continues to allow the Council to identify areas of vulnerability and information risk. It also allows it to develop and introduce policies, processes, and or training in order to reduce the likelihood of the vulnerability being exploited and causing a serious breach of the data protection legislation, or affecting the integrity and availability of important information assets.

5.10 A breakdown of service area & information security incidents types is provided at appendix 2.

5.10.1 Those service areas reporting the highest numbers of information security incidents are those processing greater volumes of personal and special category data.

6. **Information requests & internal reviews**

6.1 There were 1,420 information requests, covering the Freedom of Information Act (FOI) 2000, Environmental Information Regulations (EIR) 2004, or the General Data Regulations Subject Access Request (SAR) information regimes, this is against 1,212 last year, an increase of nearly 15%

6.2 Compliance rates overall have decreased

- FOI 1,260 requests, with 76% compliance rate at year end; compliance down by 6%.
- EIR 70 requests, with 78% compliance at year end; compliance down by 9%

- GDPR SARs 87 requests with 40% compliance at year end; compliance down by 40%

6.3 The overall decrease in compliance is due to several reasons;

- Ability of the service areas to respond to information requests tasked to them.
- Recruitment of new Information Compliance Officers during the same period of time as the biggest changes to data protection legislation in nearly 20 years.
- The need to train these staff in 3 complex legislation regimes, which continues.
- Continual checking of draft responses and disclosures prepared by new staff by experienced officers
- The loss of an experienced Information Compliance Manager, leaving a vacancy.
- The additional roles of Data Protection Officers for Powys County Council and Powys Schools being delivered by the team
- Changes to the response timescales of SARs under GDPR, from 40 days to 1 calendar month
- Organisational activity, such as restructure and redundancies.

6.4 There have been 38 requests for a review of the Council's handling of FOI & EIR requests, 27 direct from the requestor 11 from the ICO. These numbers are an increase 10.5% against last year's complaint numbers.

6.4.1 Of those 38 requests for internal review,

- 29 were due to not being satisfied with the response or the exemption applied,
- 9 because the response was late.

6.5 Of the 11 complaints referred to the ICO,

- 6 were due to the response being late. In all 6 cases the complaint was upheld
- 5 were over the provision of information or application of an exemption. 2 cases are still under consideration, 1 complaint was upheld and in 2 cases the Council's original response stood.

6.6. Additionally another 3 complaints were made to the ICO over the Council's failure to respond accordingly to those wishing to exercise their rights under data protection legislation, particularly in relation to subject access requests. In all three cases the complaints were upheld.

6.7 Also GDPR introduced additional rights of the data subject, which have to be managed and reported upon. Necessary reporting and management processes have been put in place.

6.8 Involvement of the ICO into complaints has increased from 4 last year to 5.

6.9 The ICO has previously stated that a compliance rate of at least 90% is expected.

6.10 The Information Compliance team has developed reports for service area managers in relation to the information requests received, but the structure changes resulted in further revisions to be made to the reporting process, and so these reports ceased, until the revisions can take place.

6.11 A recent exercise was undertaken to determine Powys County Council's comparison against other local authorities in Wales, since there are no central records available. There were limited responses.

6.11.1 On average 1,070 FOI requests are received by local authorities, with an average compliance rate of 85.53%. Powys County Council received 1,260 with a compliance rate of 76%

6.11.2 Most other local authorities include the reporting of Environmental Information Regulations (EIR) requests within their FOI figures. Powys records these separately, and received another 70 EIR requests with a compliance rate of 78%

7 General Data Protection Regulations (GDPR)

7.1 A separate detailed GDPR plan was developed to manage the implementation of GDPR, and those continual activities required for ongoing compliance have now been amalgamated into the IMAG.

7.2 Internal Audit considered the organisation's planning for GDPR implementation and provided a *reasonable* assurance marking, their follow up report indicated that *some significant process* had been made.

7.3 GDPR communications were delivered in via various mediums to suit a range of staff and their responsibilities towards personal data. Including to Schools, Members and also to Town and Community Councils and private companies under the Heart of Wales Business Solution provision.

7.4 A considerable amount of work was undertaken by service areas in identifying their information assets, with similar work being undertaken within ICT in mapping those technical measures in place to protect information. This work continues.

7.5 Monitoring organisational compliance with GDPR now falls under the remit of the Professional Lead Data Protection acting as the Council's mandatory designated Data Protection Officer.

7.6 The payment of data protection fees as required for both the Council and Members has been managed by the Information Compliance team.

8. Cyber Security

8.1 A dedicated Cyber Security Officer has been appointed within ICT. Cyber Security planning comprises a number of proactive actions to improve the overall security position. The plan involves the shared ICT activity with Powys Teaching Health Board.

8.2 In December 2018 Powys County Council was awarded its Cyber Essentials certification.

8.2.1 Powys County Council is currently undergoing assessment for the Cyber Essentials Plus and IASME Gold Governance certifications.

8.3 Cyber Essentials is a Government-backed, industry-supported scheme to help organisations protect themselves against common online threats. The certification enables organisations to reassure customers, partners and other business that cyber security is taken seriously, with certificate listings presented on the Government's National Cyber Security Centre web pages.

8.4 The Information Assurance for Small to Medium-sized Enterprises (IASME) was designed as a security benchmark enabling organisations to assess the level of their information security maturity, against a set of nationally recognised standards.

8.5 Powys County Council continues to meet Public Service Network (PSN) standards in order to access government responses.

8.6 Additionally the implementation of a new email system allowed the council to make use of TLS (Transport Layer Security) enabling greater encrypted email communication, especially between other local authorities and statutory organisations in Wales.

9 Resources Available

9.1 The Information Compliance team delivers the majority of the Council's information governance functions, including that of a designated Data Protection Officer, for the Council. In addition all information requests are handled, managed and responded to by the team. The team also provides the service of a designated DPO for Schools and other information governance advice under SLA.

9.2 An additional 4 Information Compliance Officers were recruited in the year, as well as the DPO for Schools. However this resulted in the loss of the Information Compliance Manager, which is still a vacant post, and is being covered by both the DPO and DPO for Schools

9.3 The recruitment of new, untrained staff at a time of the biggest change to data protection law in nearly 20 years, impacted upon the delivery of information governance practices and information requests. This impact continues to be felt as those staff continue to develop knowledge and skills in the delivery of 3 complex information legislation regimes, requiring that the more experienced officers perform checks of the work being undertaken.

9.4 Staff within the team undertake activities on a shared basis, which provides the resilience required in a small team to cover leave and other absences.

9.5 The Professional Lead Data Protection is now line managed by the Professional Lead – ICT, following the restructure and the departure of the Head of ICT.

9.6 Consideration continues to be given on the organisation's comparison with other local authorities in terms of staffing, activity and compliance.

9.7 Appendix 4 contains details of the team structure.

10. **Information Management Service**

10.1 The Information Management Service provides help and advice to all areas of the Council on information management issues including records management practices and procedures. The Service manages and stores in excess of 250,000 files of semi-current and non-current records, which are retained for a certain period of time for legal, financial, administrative or operational reasons.

10.2 During 2018/19 Information Management responded to 1,534 file requests by services across the council, 1,678 boxes of records were transferred to the Unit, at Unit 29 Ddole Road Enterprise Park, and 8,938 files were securely destroyed.

10.3 The Records Manager position has been vacant from September.

10.4 During the year the service faced a significant backlog of social care file destructions, and so to address this three temporary posts were created between November and March. At the end of the year the service still has a large backlog of file destructions and reviews, predominantly from Legal Services (8,000 files) and Social Care (9,000 files).

10.5 Due to office rationalisation the demand for file collection has been increasing which is impacting upon further limited resources.

10.6 In August 2018 Powys Teaching Health Board, (PTHB) began transferring patients' records to Unit 29 to be stored and managed through a SLA. By the end of March 2019 around 28,000 patients' files

have been transferred, generating around £8,760 for the service. PTHB continue to transfer files and the service has sufficient space in the store to continue taking records from them. In 2018/19 discussions began with the Trunk Road agency (NMWTRA) regarding the 8,000 files and plans held for them by Information Management. This is a historic arrangement with no charges made for storage.

10.7 Information Management and the Archives Service are delivered from one facility with one staffing structure. In 2018/19 the public searchroom attracted a significant increase in Archive users – both as individual researchers and group visits. A total of 3,736 visitors used the service during the year (increased from 2,246 in 2017/18). Staff responded to 820 written requests (682 in 2017/18). The Archive Service received over 100 new accessions and collections during the year. The total number of items in storage and being managed (Archives, Information Management and PTHB) is currently around 408,000.

11 Conclusion

11.1 Powys County Council continues to progress and improve its information management, assurance and governance policies, procedures, and practices. The work undertaken towards compliance with GDPR and other information legislative regimes must continue, in order to reduce information risk, likelihood of regulatory action, and to support the Council's vision of being an open and enterprising Council.

11.2 Personal data is intrinsic to much of the Council's activities, and public trust and confidence in the organisation's ability to manage and use their information appropriately is essential.

11.3 Staff awareness of information governance and compliance matters continues to improve, with a resultant rise in enquiries, requests for complex advice, requests for secure storage of records, and the nature and types of information security incidents being reported.

12. Impact Assessment

12.1 Is an impact assessment required? No

12.2 If yes is it attached? N/A

13. Corporate Improvement Plan

13.1 N/A

14. Local Member(s)

14.1 N/A

15. Other Front Line Services

15.1 Does the recommendation impact on other services run by the Council or on behalf of the Council? N/A

15.2 If so please provide their comments

16. Communications

16.1 Have Communications seen a copy of this report? No

16.2 Have they made a comment? If Yes insert here.

17. Support Services (Legal, Finance, Corporate Property, HR, ICT, Business Services)

17.1 Legal : The recommendations can be supported from a legal point of view.

17.2 Finance

17.3 Corporate Property (if appropriate)

17.4 HR (if appropriate)

17.5 ICT (if appropriate)

18. Scrutiny

18.1 Has this report been scrutinised? No

18.2 If Yes what version or date of report has been scrutinised?
Please insert the comments.
What changes have been made since the date of Scrutiny and explain why Scrutiny recommendations have been accepted or rejected?

19. Data Protection

If the proposal involves the processing of personal data then the Data Protection Officer must be consulted and their comments set out below.
N/A

20. Statutory Officers

20.1 The Solicitor to the Council (Monitoring Officer) commented as follows :
" I note the legal comments and have nothing to add to the report."

21. Members' Interests

The Monitoring Officer is not aware of any specific interests that may arise in relation to this report. If Members have an interest they should declare it at the start of the meeting and complete the relevant notification form.

Recommendation:	**Reason for Recommendation:**
That Cabinet notes and approves the report.	**The report reflects the Information Governance activities undertaken within the year.**

Relevant Policy (ies):			
Within Policy:	**Y / N**	**Within Budget:**	**Y / N**

Relevant Local Member(s):	**NA**

Person(s) To Implement Decision:	**NA**
Date By When Decision To Be Implemented:	**NA**

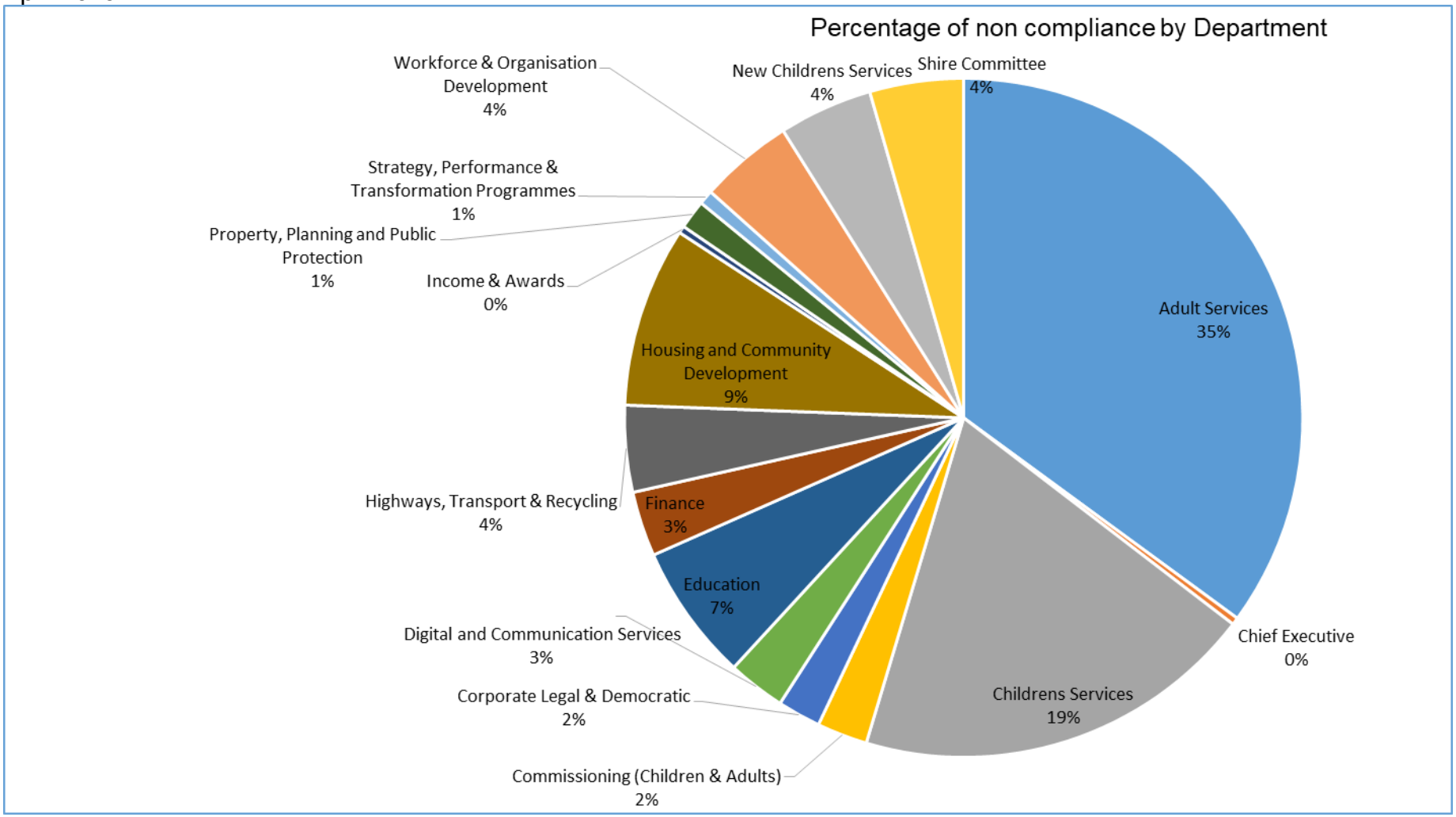
Is a review of the impact of the decision required?	**N**
If yes, date of review	
Person responsible for the review	
Date review to be presented to Portfolio Holder/ Cabinet for information or further action	

Contact Officer:	Helen Dolman Professional Lead Data Protection
Tel:	01597 826400
Email:	helen.dolman@powys.gov.uk

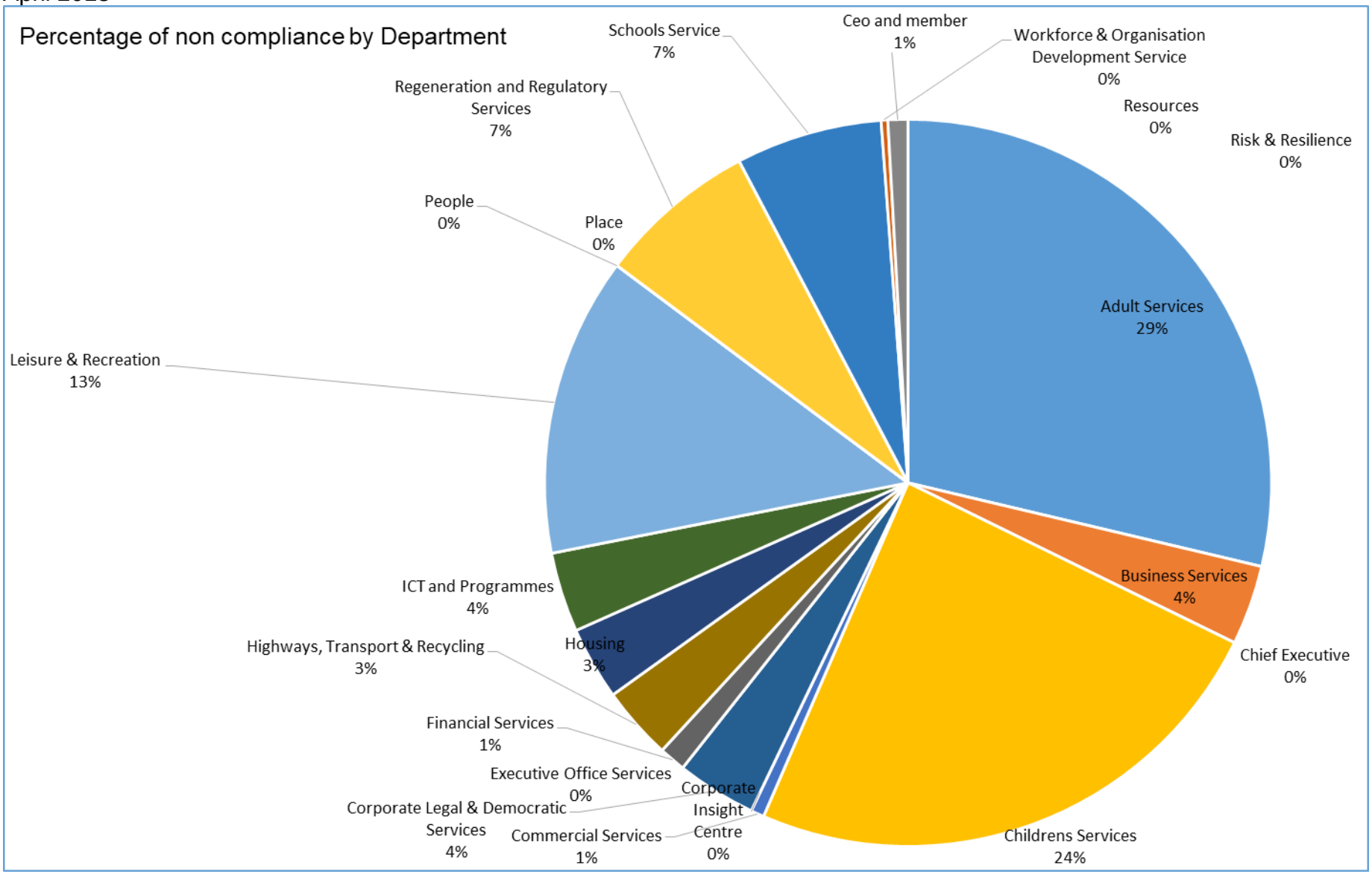
Background Papers used to prepare Report:

ICO enforcement training

April 2019



April 2018


Percentage of non compliance by Department
Schools Service 7%
Ceo and member 1%
Workforce & Organisation Development Service 0%
Regeneration and Regulatory Services 7%
Resources 0%
Risk & Resilience 0%
People 0%
Place 0%
Adult Services 29%
Leisure & Recreation 13%
Business Services 4%
ICT and Programmes 4%
Chief Executive 0%
Highways, Transport & Recycling 3%
Housing 3%
Financial Services 1%
Executive Office Services 0%
Corporate Insight Centre 0%
Corporate Legal & Democratic Services 4%
Commercial Services 1%
Childrens Services 24%

Appendix 2

Information security incident breakdown

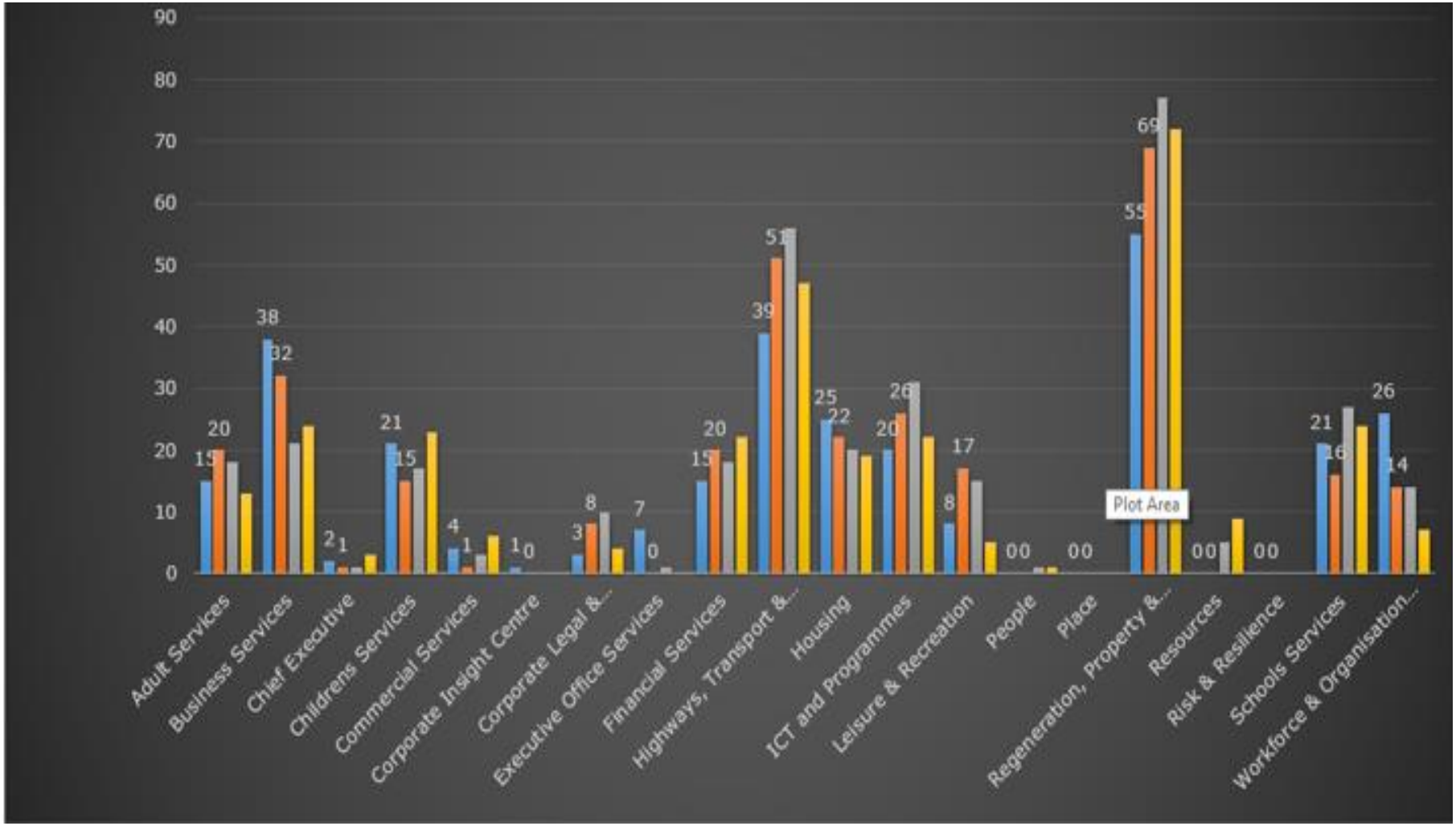
Service Area	Numbers of incidents
Adult Services	32
Business Support	3
Catering & Cleaning	2
Childrens Services	40
Commercial Services	1
Communications	2
Customer Services	6
Electoral Registration	2
Employment Services	5
Environmental Health	2
Finance	5
Housing	8
HTR	2
Human Resources	11
ICT	12
Income & Awards	10
Legal and Democratic services	8
Leisure & Recreation	3
Other controllers	7
Planning	1
Schools Services	11
Trading Standards	1
Waste	2

Type of Incident	Numbers
Bogus Caller	1
Cyber	3
Equipment	3
Inappropriate access	5
Information Rights	4
Integrity of Information	7
Loss of information	9
Misdirected external email	19
Misdirected internal email	10
Misdirected internal post	10
Misdirected external post	38
Printers	5
Storage	3
Unauthorised disclosure	58
Vacating premises	1

Information requests due each quarter by service area

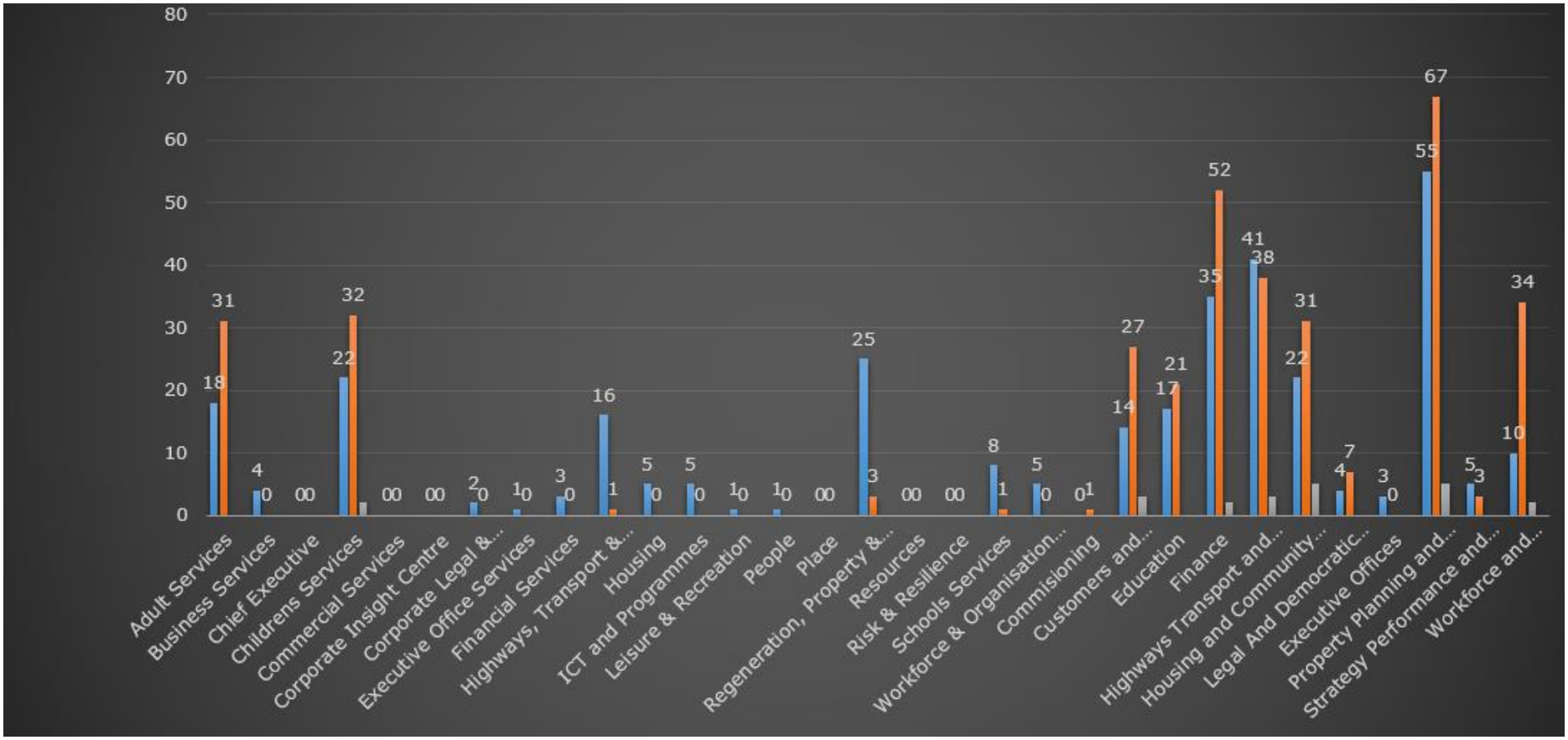
***** *Management of requests are undertaking on calendar year basis*

2018



Key –
Blue – Jan to March 2018, Orange - April to June 2018, Grey - July to September 2018, Yellow - October to December 2018

2019



Key –
Blue – Jan to March 2019, Orange - April to June 2019, Grey - July to September 2019
NB – Structure and service area name changes during the course of this reporting period has resulted in repeated service area identification through the report.

Appendix 4

Information Compliance team structure.