CYNGOR SIR *POWYS* COUNTY COUNCIL.

CABINET EXECUTIVE
21st July 2020

REPORT AUTHOR:	**County Councillor Graham Breeze** **Portfolio Holder for Corporate Governance and Engagement**
REPORT TITLE:	**Annual Information Governance Report 2019-2020**
REPORT FOR:	**Information**

1. Purpose

1.1 To brief Cabinet on the on the Information Governance (IG) activities undertaken, practices implemented, and the standards of IG compliance achieved for the financial year 2019/2020

2. Background

2.1 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.

2.2 The report is supported by the following appendices 1- 3
Appendix 1 – ICO Enforcement training graphs
Appendix 2 - Information security incident breakdown
Appendix 3 - Cost of Freedom of Information requests

3. Advice

3.1 Information Management Assurance and Governance (IMAG) Plan

3.2 The current IMAG plan was agreed by CIGG in March 2019, for implementation 2019 through to 2021. The plan details the execution of activity and objectives to improve IG practices within the Council. It also identifies and manages the ongoing IG work that takes place to maintain levels of compliance with information legislation, and standards of good practice.

3.3 There are 48 elements to the plan, as at the 31st March 2020,

- 12 had been completed,
- 24 were in progress and still within timescales,
- 3 were in progress but not likely to be completed within timescales
- 9 were out of timescales

3.4 Two CIGG meetings have taken place in the year where implementation of planned practices is considered, and challenged where timescales have not been met, and areas of concern discussed.

3.5 CIGG meets quarterly; with the August meeting cancelled and the March meeting cancelled due to priority breach management work and invoking of the Council's Business Continuity plans

3.6 Additionally, regular Corporate Information Governance Operational Group (CIOG) meetings have taken place, 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 December 2012 the Information Commissioner (ICO) issued an enforcement order against Powys County Council requiring that all staff with access to personal data undertake training in the basics of the data protection and also the organisation's information policies, every 3 years.

4.2 The ICO regularly recommends to organisations that training should be completed on an annual basis. Additionally, the general rise of cyber security threats creates a new risk to the Council.

4.3 In April 2019 the Council amended its training requirements to include cyber security, reflecting those messages within the Council's information policies and revised data protection information.

4.4 All staff, agents, members etc with access to personal data and / or ICT equipment must undertake the mandatory *Cyber Security and GDPR* training, on an annual basis. Thus, exceeding the requirements of the ICO enforcement order. CIGG directed that all would complete this training between its release in April 2019 and the 31st March 2020.

4.5 Monthly reports have continued for Heads of Service and Executive Directors identifying those staff who are non-compliant, in order that they take necessary action to ensure compliance for their service area(s)

4.6 Compliance details (Departmental breakdowns at Appendix 1)

**	2nd April 2019	2nd March 2020*	2nd April 2020**
Number of staff requiring training	2,188	2,453	2,391
Number of staff trained	1,889	2,356	1,812
Compliance rate	86.33%	96.05%	75.78%
Target Compliance rate	95%		

* mixture new and old courses

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

4.9 The decrease in the March to April figures is attributed to the decision that all were to have completed the new Cyber Security and GDPR training,

by the 31st March 2020, irrespective of the renewal period of the old training courses. As such the records for old training courses we no longer taken into account.

4.10 In August 2019 an agreed escalation process was implemented in respect of those who had persistently (over 3 months) remained non-compliant with the training requirements. Where, following a specific reminder to them and their line manager they remained non-compliant, their ICT access was to be removed. The execution of the escalation process was cancelled, by the SIRO.

5 Information Security Incidents

5.1 The council has had robust personal data breach reporting and management processes in place, for a number of years, which continues to ensure swift containment action, informed identification of information risks and mitigation, and supports the regulatory reporting requirements, to both the regulator and data subjects.

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

	2018/2019	**2019/2020**
Numbers of reported incidents	176	230
Number of personal data breaches	71 *	104*
Number of incidents reported to the ICO	25	9 (*1 by another organisation in respect of PCC data*)
Number of notifications to data subjects	11	18
Number of separate complaints made to the ICO over personal data breaches	3	4
Number of DPA breaches occurring externally	52	68
Number of DPA breaches occurring internally	17	21
Number of DPA breaches involving sensitive personal data	22	32
Number of DPA breaches contained	56	80

* 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 A breakdown of service area & information security incidents types is provided at Appendix 2.

5.4 The increase of personal data breaches can likely be attributed to a greater staff awareness of the need to react to the incidents and breaches that occur, following media and press interest in the potential fines with the implementation of GDPR. The decrease of notifications to the ICO can be attributed to greater clarity from the regulator as to what would constitute a

reportable breach. Awareness is raised through CIGG, CIOG and messages to staff.

5.5 Reports of information security incidents are regularly made to CIGG, and CIOG and staff are made aware of the need to report incidents and breaches through notices and reminders in relation to the incidents that have occurred

5.6 Those personal data breaches reported to the ICO include the disclosure of information through various means, such as failing to remove (redact) relevant information, misdirected emails, failing to add privacy measures, and provision of information to those not entitled to receive it.

5.7 In all but one case the ICO has found that the Council breached data protection legislation, though has recognised that in most cases this has been due to human error in failing to follow organisational measures put in place to prevent breaches of personal data, rather than the Council not having necessary measures in place.

5.8 Whilst no regulatory action, such as fines or enforcement orders, have been taken against the Council, where the ICO has recommended further improvements, such as service specific or general awareness, checking processes employed, then these are implemented by the relevant service area or organisation as appropriate.

5.9 The ICO has provided 33 recommendations, within their decision notices. At this time, 26 have been implemented, 4 partially implemented and 3 not yet implemented. The implementation of recommendations maybe part of wider pieces of work, which have been delayed due to COVID work.

5.10 There has been an increase in the numbers of complaints made directly to the ICO, since the public have become much more aware of their information rights following the implementation of the General Data Protection Regulations.

5.11 The four complaints to ICO relate to disclosure of information, loss of information and the medium used to transfer information. In two of the four cases, no breach of personal data had occurred. Where the Council was found to have breached personal data then recommendations for improvements were made.

5.12 The reporting and management of information security incidents and personal data breaches also allows the Council to identify areas of vulnerability and information risk, enables the development and introduction of relevant policies, processes, and or training in order to reduce the likelihood of the vulnerability being further exploited and causing a serious breach of the data protection legislation, or affecting the integrity and availability of important information assets.

5.13 Care has been taken to ensure that the cyber security and information compliance areas complement each other when responding to cyber incidents which also affect personal data.

6 Information Requests

6.1 There were 1,295 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 1,420 last year, a decrease of 9%

6.2 The Information Commissioner has indicated that she expects a 90% compliance rate.

Information Regime	Numbers received	Compliance rate	Compliance up or down
FOI	1095	69%	↓ 9%
EIR	118	58%	↓ 25%
SAR	82	29%	↓ 27%

6.3 Where records indicate reasons for non-compliance with FOI/EIR timescales, then

- 63% of non-compliance was due to late provision of information to the Information Compliance Team, by the service Area(s)
- 14% of non-compliance was due to late approval of the drafted response by the Head of Service(s) or their designated deputy
- 20% of non-compliance was due to delays by the Information Compliance Team themselves. Such as large complex requests requiring inspection, redaction and /or decisions over the application of exemptions.

6.4 Based on the above then had the only delays experienced been down the to the Information Compliance Team then the organisational compliance rate for FOI/EIRs could have been around 94%

6.5 Reports detailing reasons for lateness, service area(s) involved and impact of such were reported to Senior Leadership Team for quarters 1 and 2. Lack of resources prevented the same for quarter 3.

6.6 The continued decrease of compliance rates can be attributed to.

- Delayed provision of information from the service areas to enable a response to the information requests tasked to them. Going forward both the organisational compliance rate and the reasons for noncompliance will be reported to CIGG and Service KPIs
- The loss of 40% of Information Compliance Officers (3 out of 5) in the year. Recruitment was further delayed due to COVID 19
- The ongoing need for internal training in complex information legislation, and which will continue

- Continued checking of draft responses and disclosures prepared by less experienced staff by more experienced officers.
- Absence of dedicated Information Compliance Manager in post for most of the year, which has now been filled.

6.7 Many SARs involve large volumes of files, records, emails, documents etc, which have to be examined and considered for disclosure, redacting information where not appropriate for disclosure or not the personal data of the requester. As such these produce a great deal of printed material, sometimes over four boxes worth of information, or 1,000s of emails.

6.8 The time limits for SARs is one month with an additional two months available in where the case is complex. However, the regulator is clear that volume is not related to complexity.

6.9 Details of complaints over information requests

Complaint to Powys County Council – internal review	**36**	**Complaint made directly to the ICO**	**7**
Over lateness	11		4
Over handling of request	9		3
Application of exemption	16		
ICO involvement in internal review	3		
Outcome – complaint not upheld	9		1
Outcome – complaint upheld	9		5
Outcome – complaint partially upheld	8		
Withdrawn			1
Still under consideration at 31-03-20	10		

6.10 During the year, the Information Compliance Team

- Commenced a project looking to move from a paper-based process of undertaking SARs – this work ceased with the loss of staff from the Team.
- Commenced a project with Business Intelligence to look at automating information request processes and reporting, and service management dashboard reporting – this work continues
- Revisited its tasking and chasing processes in an attempt to obtain information from the service area(s) within timescales.
- Developed staff objectives to improve knowledge and skills in dealing with information requests and personal data breaches.

6.11 A cost analysis exercise of FOI/EIR requests for March 2019 was undertaken, considering the time spent and the likely costs to the organisation. The cost of FOI requests to Powys County Council briefing report is provided at Appendix 3

7 Resources Available

7.1 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. All formal 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, to every school.

7.2 The Team is to comprise of 5 Information Compliance Officers, 1 Information Compliance Manager, 1 Data Protection Officer Schools, and 1 Professional Lead Data Protection.

7.3 However, 3 of the 5 Information Compliance Officers left, the Information Compliance Manager post has been vacant until March 2020, the Data Protection Officer Schools post has been vacant since March 2020. The Professional Lead Data Protection undertakes both DPO and IG activities, in addition to the roles of Regulation of Investigatory Powers Act 2000 (RIPA) Co-ordinator, and Senior Responsible Officer for Camera Surveillance

7.4 A business case was made for a review of the Team, which identified resources required, and the cost of such, and identified changes possible within current budget. It has been agreed that the review can take place in line with the current budget.

8 Data Protection Officer

8.1 All public authorities are required to have in place a designated Data Protection Officer whose position and tasks are detailed within data protection legislation

8.2 In addition to the provision of advice and support, the DPO undertakes its monitoring responsibilities through reporting processes, working closely with service areas, development of information asset registers which act as records of the Council's processing activities, managing the mandatory assessment of data protection risks for new ways of working or projects (Data Protection Impact Assessment) etc

8.3 The DPO over sees the reporting, investigating and management, of personal data breaches and where the breach is of such seriousness undertakes the necessary investigations.

9 Cyber Security

9.1 The ICT Cyber Security Officer delivers a joint service under the Section 33 agreement with Powys Teaching Health Board.

9.2 In August 2019 the Council achieved Cyber Essentials Plus and IASME accreditations.

9.3 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.

9.4 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.

9.5 The Major Incident procedures have been approved, which advise on the response to and the management of any major ICT systems incidents, and which are aligned to the revision of the Information Security Incidents procedures which cover breaches of personal data.

9.6 The cyber response plan is in the process of being drafted which will then complement the above procedures, and will also outline the steps to be taken to prevent cyber-attacks, detection processes, and the procedures to be followed should these attacks occur.

9.7 Establishment of closer working relationships with Civil Contingencies and Emergency Planning Officers for the purposes of response to major ICT incidents, which may affect the wider organisation such as cyber security attacks, or emergency situations. Including joint attendance at nationally organised multi agency cyber exercises.

10 Schools DPO Service

10.1 The Information Compliance Team also deliver DPO duties and IG support for each of the Schools in Powys, rather than each having to designate their own DPOs.

10.2 Again, this has consisted of advice, checking on fee payments, management of personal data breach processes, DPIAs. The DPO Schools has also undertaken a range of audits in respect of a school's compliance with data protection legislation with findings being fed back to the school.

10.3 The DPO Schools post has been vacant since March 2020, with the duties being shared between the Information Compliance Manager and the Professional Lead Data Protection.

11 Information Management Service

11.1 The service delivers the secure storage of the Council's inactive hard copy records, and information will be provided as soon as possible. The service is currently experiencing reduced capacities due to the current situation once staff return from redeployment due to COVID 19 work. CIGG have been made aware of the difficulties

12 Conclusion

12.1 Powys County Council continues to take steps to progress and improve its information management, assurance and governance policies, procedures, and practices. The work being undertaken towards compliance with data protection legislation 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.

12.2 Falling information request compliance rates, increases the organisational risk of regulatory action, which is not purely attributable to the Information Compliance Team and requires a corporate response in order to improve those compliance rates, taking into account any decreases of information requests due to Covid and also planning and monitoring of recovery by CIGG

12.3 The ability to retain staff within the Information Compliance Team is vital in order for all team members to be able deliver a range of IG services to the Council and Schools, thus releasing more senior team members to concentrate on delivering new IG initiatives and projects.

12.4 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.

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

12.6 Senior Information Risk Owner's statement of assurance.
Partial Assurance - We are able to offer partial assurance that the council's arrangements adequately reflect the principles of good information governance. Some key risks are not well managed, and processes require the introduction or improvement of internal controls to ensure effective governance, but plans for future improvement are in place and are monitored by CIGG

13 Planned Activity 2020-2021

- Continue the review of the Information Compliance Team, including roles, grades, and numbers to take place, in line with budget limits.
- Recruitment of vacant posts to recommence – (*this was stalled due to COVID 19)*
- Introduce new measures identifying reasons for FOI& EIR noncompliance
- Recommence electronic SAR project
- Continue automation of information requests processes and reporting, including automated chasing and recording of non-compliance rates and reasons, and provision of information directly to management dashboards
- Continue to monitor training compliance rates utilising escalation processes, where necessary

- Progress, with Business Intelligence, the publication of self-service data sets, based on regularly asked FOIs.
- Continued implementation of IMAG plan
- Continue close working relationships with cyber security staff to ensure both technical security standards and information governance issues are addressed in tandem

14. Legal implications

14.1 Legal; the recommendations can be supported from a legal point of view

14.2 The Head of Legal and Democratic Services (Monitoring Officer) notes the report and has nothing further to add.

15. Data Protection

15.1 The Data Protection Officer notes the content of this report and has nothing further to add.

16. Comment from local member(s)

16.1 NA

17. Integrated Impact Assessment

17.1 NA

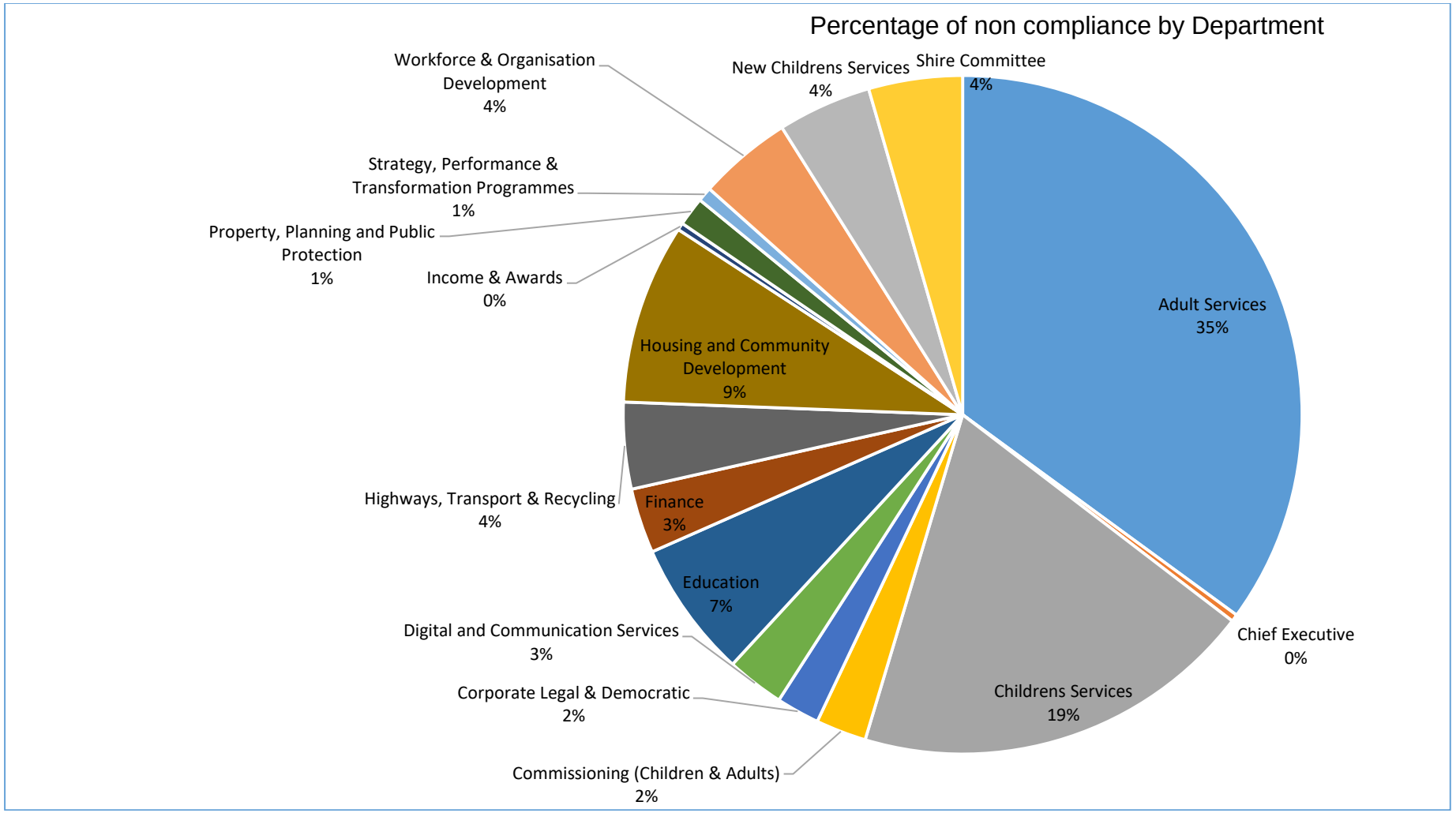
18. Recommendation

18.1 Cabinet notes the assurance set out in 12. 6 and the planned activity for 2020-2021 as set out in paragraph 13.

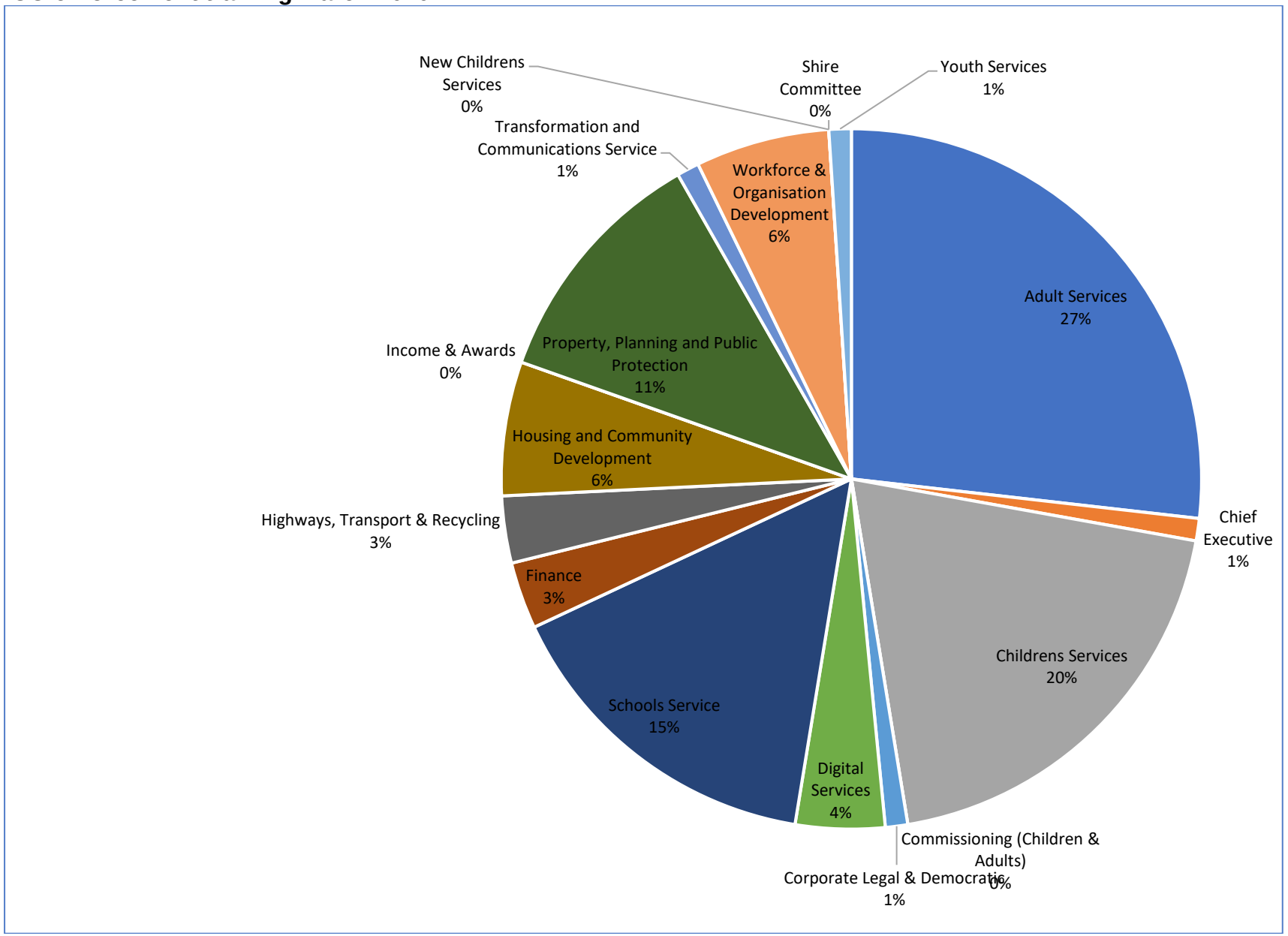
Contact Officer: Helen Dolman Tel: 015697 826400 Email: helen.dolman@powys.gov.uk Head of Service: Diane Reynolds Corporate Director: Ness Young

Appendix 1

ICO enforcement training April 2019



ICO enforcement training March 2020



Appendix 2

Information security incident breakdown

Service Area	Numbers of incidents
Adult Services	24
Business Support	1
Catering & Cleaning	3
Childrens & Adults	2
Childrens Services	45
Commissioning	2
Community Safety Partnership	1
Corporate	2
Customer Services	3
Development Control	17
Digital Services	16
Employment Services	10
Environmental Health	3
Finance	3
Housing	9
HTR	2
Human Resources	10
Income & Awards	21
Legal and Democratic services	6
Members	1
Not Known	6
Occupational Health	2
Other controllers	14
Powys Registrations	1
Powys Youth Justice	2
Property Services	3
Schools Services	17
Trading Standards	3
Transport	1
Waste	2
Workforce	1

Type of Incident	Numbers
Complaint	17
Cyber	1
Inappropriate access	3
Information Rights	3
Integrity of Information	12
Loss of information/equipment	12
Misdirected external email	16
Misdirected internal email	26
Mis-handling information	19
Printers	19
Unauthorised disclosure	102

Appendix 3

Cost of Freedom of Information requests

The cost of Freedom of Information requests made to the Council has been raised on many occasions, and with local authorities handling requests differently there is little information available as to the true costs of responding to FOIs.

In an attempt to establish some costings, the Information Compliance team undertook an exercise in early 2019, as to the time taken on each step of the process in handling a FOI request.

These steps, being the time taken to

- Undertake request administration
- Provide assistance and advice on requests
- Task the request to the service area
- Locate the information
- Retrieve the information
- Extract the information
- Gather information
- Research
- Draft response
- Check draft response
- Carry out Head of Service Checks

Service areas were requested to complete cost analysis sheets for each request tasked to them. However, the responses received from the service areas was very limited. 115 requests and only 16 response.

As such, multipliers were then attributed to the figures provided to develop appropriate data for each task, based upon the average of time taken per task.

Based upon the data received and the multipliers used then it can be determined that approximately 528 hours were spent by staff of Powys County Council dealing with FOIs in March 2019

In terms of cost then this would be based upon the pay scale of each member of staff involved. However, the grades of staff dealing with FOIs vary between Grade 5 to HoS at Senior Manager grade.

In applying the cost limit to a FOI request to consider if it exceeds costs under the Appropriate Fees and Limits Regs then the figure of £25 per hour is used; as such using this same hourly rate this then equates to

- £13,196 cost for the month of March, (at 115 requests for the month) or
- £158,400 for the year, based on the above (115 x12) or
- £144,585 for the year using the numbers of FOIs received in 2018 (1260 received)
- £114.75 per request.
- Each request taking an average of just over 4 ½ hours work

A report from MySocoiety.org[1] into FOIs, stated that “Examining over 250 responses from councils on WhatDoTheyKnow[2] shows the difficulty in trying to find a cost per FOI requests. Itemised values range from £12 to £450”

Caveat

With the low number of responses provided then the data can only be based on that received and multiplied accordingly to obtain an overall monthly figure. To develop more precise figures, would require a greater level of information from the service area, and can only be based upon that information supplied.

[1] https://research.mysociety.org/publications/freedom-information-local-government
[2] https://www.whatdotheyknow.com/