CYNGOR SIR *POWYS* COUNTY COUNCIL.

CABINET EXECUTIVE

REPORT AUTHOR:	**County Councillor Beverley Baynham, Portfolio Holder for Corporate Governance and Regulatory Services**
REPORT TITLE:	**Annual Information Governance Report 2020-2021**
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 2020/2021

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 This report is supported by the following appendices,

- Appendix 1 – ICO Enforcement training graphs
- Appendix 2 - Information security incident breakdown

3. Information Management Assurance and Governance (IMAG) Plan

3.1 The 2019-2021 IMAG plan was agreed by the Corporate Information Governance Group (CIGG) in March 2019. 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.

3.2 In December 2021, CIGG agreed a revision of timescales due to the impact of COVID 19, and IG work undertaken in support of the Council's response to COVID 19 and Test Trace and Protect (TTP) work both for Powys County Council and on a wider national basis.

3.3 As at the 31st March 2021 there were 50 elements to the plan,

- 16 had been completed (32%),
- 27 were in progress and still within the revised timescales (54%),
- 7 were out of timescales (14%), which included the elements of Information Asset Registers, controls when working with others, review of the Corporate Retention Schedule, computer system audit

functionality, Council constitution changes, review of the Terms of Reference of the Information Governance groups, and relevant training for Information Asset Owners (IAO) /Senior Information Asset Owner (SIRO)

3.4 Four 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, and actions required identified. These meetings are chaired by the SIRO

3.5 CIGG meets quarterly; and within the year returned to routine meetings as described with its Terms of Reference.

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

3.6 CIOG meets every 6 weeks, and again meetings have returned to routine scheduling.

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 In April 2019 the Council amended its training requirements, to be undertaken on an annual basis, and to include cyber security, reflecting those messages within the Council's information policies and revised data protection information.

4.3 In April 2021 the reporting for training was transferred from the Information Compliance team to the Business Intelligence team, to enable the provision of compliance data to managers within dashboards, alongside other mandatory training reports.

4.4 Compliance details (Departmental breakdowns at Appendix 1)

	2nd March 2020*	2nd April 2020	1st April 2021**
Number of staff requiring training	2,453	2,391	3015
Number of staff trained	2,356	1,812	2314
Compliance rate	96.05%	75.78%	76.7%
Target Compliance rate	95%		

* Mixture of new and old courses
** Change to a different reporting process

Overall training compliance figures continue to form part of the IG measurements provided to CIGG.

4.5 The decrease in organisational compliance rates and the increase of noncompliance within HTR can be attributed to the decision to include HTR staff within the training requirement due to the rollout out of in cab technology, but due to the jobs undertaken normal E learning was not feasible and so face to face training was implemented, but due to COVID 19 this has been greatly reduced. However due to the limits of the devices and the information contained within them, then it was considered appropriate to tolerate this risk.

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 relevant reporting obligations, 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.

	2019/2020	2020/2021
Numbers of reported incidents	230	220
Number of personal data breaches	104*	115*
Number of incidents reported to the ICO	9 (1 by another organisation in respect of PCC data)	7
Number of notifications to data subjects	18	5
Number of separate complaints made to the ICO over personal data breaches	4	3**
Number of DPA breaches occurring externally	68	70
Number of DPA breaches occurring internally	21	44
Number of DPA breaches involving sensitive personal data	32	20
Number of DPA breaches contained	80	89

* 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.

** challenged regulator over data subject(s) ability to raise complaint, still awaiting a response.

5.3 A breakdown of service area & information security incident types is provided at Appendix 2.

5.4 Whilst there has been a slight decrease in the number of information security incidents reported there has been an increase of personal data breaches occurring (11%), it is likely that this increase can be attributed to changes in working locations/conditions, duties, and delivery of new and changed services due to COVID. Those that reach the threshold of needing to be reported to the ICO remain reasonably static.

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. Additionally, the Information Security Incident and Personal Data Breach reporting policy and procedures were revised and re-presented to staff.

5.6 Those personal data breaches reported to the ICO include a cyber-attack on one of the Council's providers, disclosure of information through various means, such as including information within shared reports, misdirected emails, local caching of information, and failing to redact information.

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 the necessary measures in place.

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

5.9 The ICO has provided 27 recommendations, within their decision notices. At this time, 17 have been implemented, and 10 not yet implemented. The implementation of recommendations maybe part of wider pieces of work, which have been delayed due to COVID work.

5.10 Some recommendations are repeated within ICO decisions.

5.11 The three complaints to ICO relate to disclosure of information. In two of the three cases, a breach of personal data had occurred. Where the Council was found to have breached personal data then no further recommendations for improvements were made.

5.12 In the third case the decision as to whether a personal data breach occurred was made without affording the Council the opportunity to respond to the complaint made. The Council continues to challenge this decision and the ability of the data subject to raise the complaint made to the ICO.

5.13 The reporting and management of information security incidents and personal data breaches continues to allow 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.

5.14 Processes in place 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 1000 valid information requests covering the Freedom of Information Act (FOI) 2000, Environmental Information Regulations (EIR) 2004, or the UK General Data Regulations Subject Access Request (SAR) information regimes, this is against 1295 last year, a decrease of 23%

6.2 The decrease can be attributed to COVID 19, and requestors understanding the additional burdens placed on public authorities. Whilst the ICO initially indicated they would be a pragmatic regulator during these times, the timescales in responding to these information requests could not be changed without changes to the legislation itself.

6.3 The Information Compliance team continued to deliver services throughout this time and attempted to release some pressure on the service areas by attempting to gather relevant information where it was possible to do so.

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

Information Regime	Numbers received	Compliance rate	Compliance up or down
FOI	789	86%	+17%
EIR	143	94%	+36%
SAR	68	87%	+28%
Overall	1000	85%	+20%

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

- 80% of non-compliance was due to delays by the service areas.
- 15% of non-compliance was due to delays by the Information Compliance Team themselves. Primarily due to large complex requests requiring inspection, redaction and /or decisions over the application of exemptions.
- 5% of non-compliance was due to other factors, such as the impact on COVID 19.

6.6 Based on the above then had the only delays experienced been by the Information Compliance Team then the organisational compliance rate for FOI/EIRs could have been around 97%.

6.7 Reports detailing reasons for lateness, were supplied to CIGG.

6.8 These figures do not apply to UK GDPR SARs since the delays experienced are predominantly due to the Information Compliance team. Most

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.

6.9 Due to the imposed new ways of working then it has been necessary to develop and implement electronic processes for responding to UK GDPR SARs. To modify the transfer of information from the Services, to create electronic versions, of documents, since many SARs still involve manual records, and to make the disclosure to the individual electronically as well.

.

6.10 The improved compliance rates can be attributed to

- Reduced number of information requests
- Recruitment during the year to the vacancies that had been created in the previous year, by the loss of staff.
- Filling the vacant Information Compliance Manager post, however this had a knock-on effect on the DPO for Schools post.

6.11 Details of complaints over information requests

Complaint to Powys County Council – internal review	**24 (↓12)**	**Complaint made directly to the ICO**	**2 (↓5)**
Over lateness			2
General disagreement with response	15		
Application of exemption	9		
Outcome – complaint not upheld	5		
Outcome – complaint upheld	1		2
Outcome – complaint partially upheld	2		
Withdrawn	6		
Still under consideration at 31-03-21	10		

6.11 During the year, the Information Compliance Team,

- Was not able to continue with the project to develop automated information request processes and reporting, and service management dashboard reporting. This work has re-commenced at the start of the 21-22 year.
- Recruited two new members of staff, who commend home working from the start of their employment with Powys County Council, and which also includes the training on handling information requests and other IG activities.

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, and a DPO for Schools Service. All formal information requests are handled, managed, and responded to by the Team.

7.2 The Team would normally be comprised of 5 Information Compliance Officers, 1 Information Compliance Manager, 1 Data Protection Officer Schools, and 1 Professional Lead Data Protection.

7.3 However, with 3 of the 5 Information Compliance Officers leaving in 19-20, and the subsequent impact of the COVID pandemic and lockdown then the recruitment of 2 new Information Compliance Officers was not finalised until the summer of 2020. The previously vacant post of Information Compliance Manager was filled in March 2020, but this left the DPO Schools post vacant.

7.4 From April 2020 to August 2020 one member of staff was redeployed on COVID work.

7.5 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.

7.6 A review of the Information Compliance team has been undertaken in light of changes required to the team and also for the budget savings required. These changes are currently under consultation.

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 providing advice & support, 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 ensures notification to the ICO, and if required undertakes the necessary investigations.

9. Cyber Security

9.1 The ICT Cyber Security Manager delivers a joint service under the Section 33 agreement with Powys Teaching Health Board. A Cyber Security Officer has also been recruited to assist with this growing area of work.

9.2 In November 2020 the Council achieved Cyber Essentials Plus and IASME Gold 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.

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. IASME Gold accreditation involves on site audit on the level of information security provided by the organisation.
The Council continues to achieve its PSN compliance status, allowing the sharing of Data with Central Government departments such as the DWP.

9.5 During the Covid Pandemic, the Cyber Resilience programme has proven effective in preventing any major Cyber Security incident from impacting on the work of the Council. The Council was prepared for and continues to provide a safe and secure ICT provision for staff to work from home. Cyber Aware bulletins have been issued during this time to staff in order to inform and raise their awareness of the current Cyber Security threat.

9.6 The Welsh Government have been proactive in providing 3 rounds of funding for Cyber Resilience during the financial year. Powys County Council has used their funding to provide tailored training courses for the recently recruited Cyber Security Officer as well as obtaining a professional Qualification (CISSP) for the Cyber Security Manager. Further funding has been used to invest in additional Cyber Resilience tools to protect against ransomware attacks and a programme of work to increase training and awareness for all staff on the threat of Phishing emails.

9.7 The Cyber Response plan continues to be developed and will be a key part of the Cyber Resilience Strategy.

10. DPO for Schools Service

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

10.2 The Head of Schools Services is provided with an annual DPO for Schools report, in line with the school year. The 2019-2020 report having been issued in October 2020.

10.3 From September 2019 to March 2020 this work has consisted of over 370 separate pieces of data protection, and information governance advice, for example on information sharing, security of pupil work through the use of Apps, on-line teaching queries, information requests, and also in support of personal data breaches, and Data Protection Impact Assessments.

10.4 Only one personal data breach involving a School met the threshold for reporting to the ICO.

10.5 Work of the DPO schools is included within reports to CIGG quarterly, even though for the purposes of data protection they are separate controllers.

10.6 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 Throughout the pandemic and as the Council invoked its Business Continuity Plan, staff have been on site 5 days a week, as it was felt important to continue file retrievals for those council services who continued to operate. Information Management also store and operate a records management service for PTHB, and again it was considered essential that file requests were processed as quickly as possible. On one day alone in January 2021 they requested over 100 patient files from store.

11.2 Staffing issues have plagued Archives and Information Management for over 18 months and has prevented the provision of management information to CIGG. Attempts have been made to recruit a second archivist (in addition to the Professional Lead Arts and Culture) since January 2020. This has created significant pressures on staff time, with tasks such as cataloguing and accessioning of new archive collections being put on hold as the remaining staff focus capacity on day-to-day responsibilities.

11.3 During the year the service has commenced a specific piece of work with some service areas in relation to the retention and deletion of both hard copy and corresponding electronic records.

12. COVID/TTP

12.1 The impact of the pandemic has resulted in

- All members of the Information Compliance Team working from home, including the newly recruited staff.
- The planned movement from manual SAR work to electronic had to be escalated and implemented quickly. This implementation work remains ongoing to ensure solutions developed are robust and secure.
- A slight reduction in information requests received, and whilst the ICO indicated initially that they would be a pragmatic regulator, the legislation around response timescales did not change, and so this service had to be maintained. Additional support was provided to the service area in the identification of relevant information to enable the Council to respond to these requests.
- An assessment of the Council's ability to recover from the result of the pandemic on information requests, having been undertaken. Which due to the continued activity during the year has not resulted in any great recovery work being required, but which has enabled a review of current practices and identification of further improvements required, such as improved training on information requests for staff and members.

- The continued need to ensure the management and investigation of information security incidents and personal data breaches, and responses to those wishing to exercise their data protection rights.
- Involvement in local and national groups considering and managing the data protection issues around the use of personal data to support the NHS Test Trace and Protect service, and the Council's wider response to COVID issues, such as information sharing agreements, analysis and development of dataflows, and Data Protection Impact Assessments.

13. Conclusion

13.1 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.

13.2 The impact of the Information Compliance team reorganisation and budget savings will need to be monitored.

13.3 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.

13.4 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.

13.5 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.

14. Planned Activity 2021-2022

- Implement the changes to the Information Compliance Team, including changes to roles, grades, and numbers, in line with new budgetary requirements, and to also assist staff in the delivery of these revised roles, thorough training and support.
- Continue with full implementation of the electronic SAR project.
- Continue with the development of automated information requests processes and reporting, including chasing and recording of non-compliance rates and reasons, and provision of information directly to management dashboards.
- Continue to monitor training compliance rates.

- Progress, with Business Intelligence and also the relevant services, the publication of self-service data sets, based on regularly asked FOIs, including information request statistical information.
- Continued implementation of IMAG plan, in particular the review of work previously undertaken on Information Asset Registers
- Continue close working relationships with cyber security staff, to ensure both technical security standards and information governance issues are addressed in tandem.

15. Legal implications

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

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

16. Data Protection

16.1 The Data Protection Officer is the author of this report and has nothing further to add.

17. Comment from local member(s)

17.1 NA

18. Integrated Impact Assessment

18.1 NA

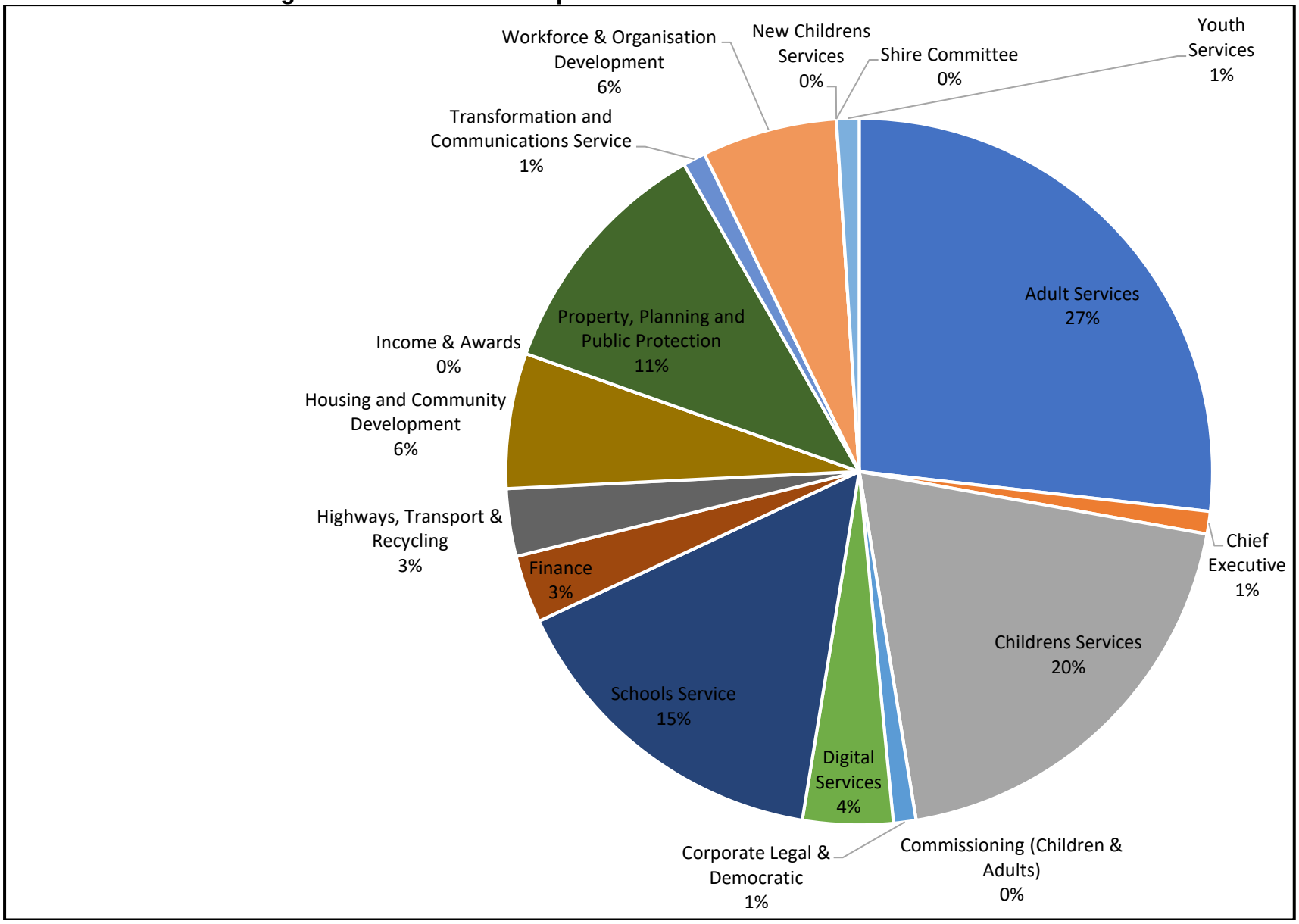
19. Recommendation

19.1 Cabinet notes the assurance set out in 13.5 and the planned activity for 2021-2022 as set out in paragraph 14.

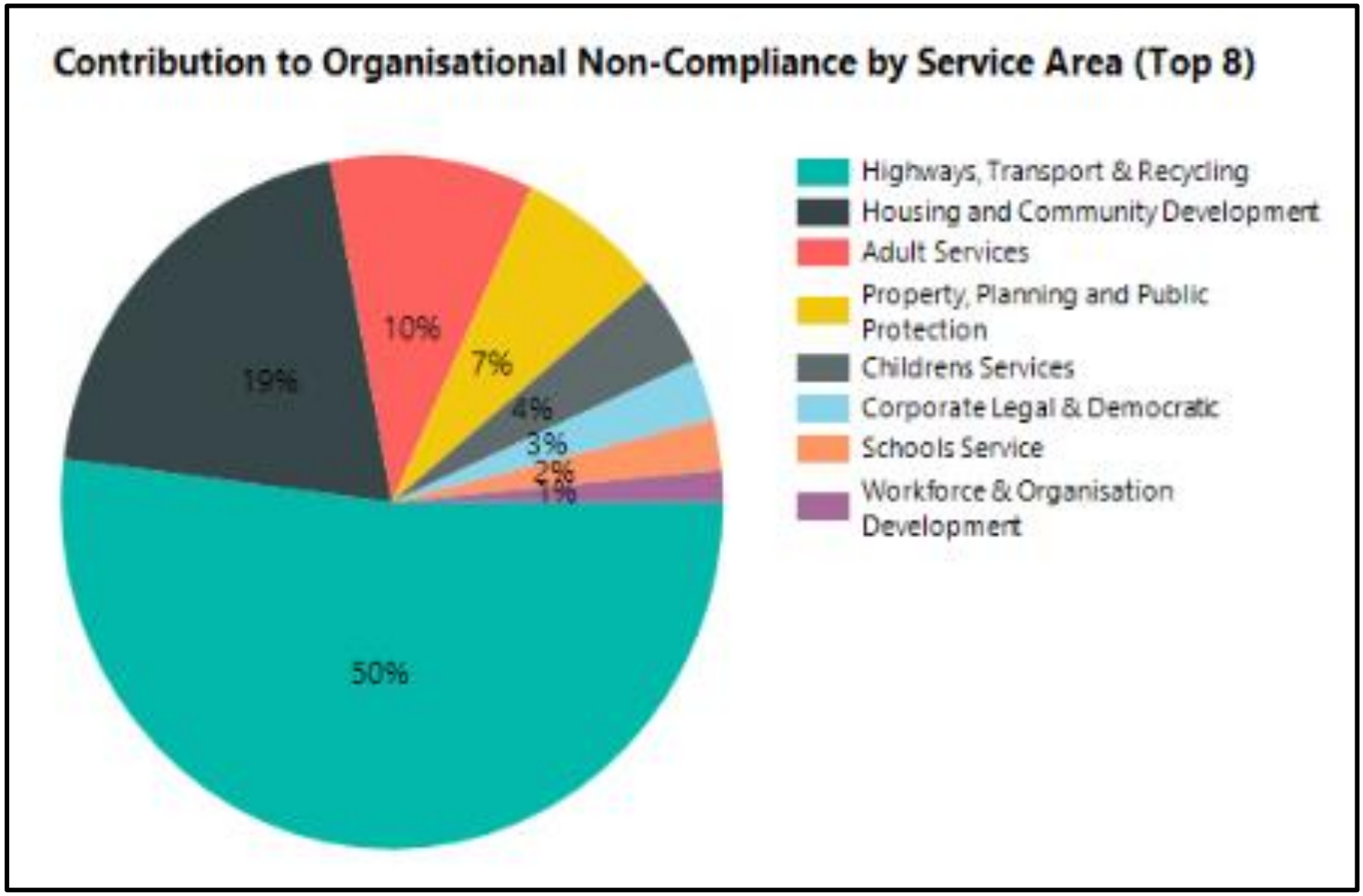
Contact Officer:	Helen Dolman
Tel:	015697 826400
Email: helen.dolman@powys.gov.uk	
Head of Service: Diane Reynolds	
Corporate Director:	Nigel Brinn

Appendix 1

ICO enforcement training March 2020 – noncompliance



Cyber Security and GDPR Training April 2021



Appendix 2

Information security incident breakdown

Service Area	Numbers of incidents
Adult Services	37
Childrens Services	76
Commissioning	7
Digital Services	14
Finance	16
Housing & Community Development	9
HTR	6
Legal and Democratic services	8
Members	1
Other	3
Property, Planning and Public Protection	17
Schools Services	16
Workforce & organisational Development	10

Type of Incident	Numbers
Complaint	18
Cyber factor	6
Inappropriate access	7
Inappropriate processing of data	11
Information rights	5
Integrity of information	5
Loss of information	2
Loss/theft of equipment	1
Other	10
Physical Security	2
Unauthorised disclosure (External)	100
Unauthorised disclosure (Internal)	53