CYNGOR SIR *POWYS* COUNTY COUNCIL.

CABINET EXECUTIVE
Date: 20th December 2022

REPORT AUTHOR:	**County Councillor Jake Berriman, Cabinet Member for a Connected Powys.**
REPORT TITLE:	**Annual Information Governance Report 2021-2022**
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 2021/2022

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 2021-2023 IMAG plan was agreed by the Corporate Information Governance Group (CIGG) in March 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.

3.2 As of the 31st of March 2022 there were 61 elements to the plan,

- 23 had been completed (38%), Such as the development and release of training over the investigation of personal data breaches, development of an action plan in response to SWAP report on the Council's management of electronic information, implementation of electronic Subject Access Request (SAR) processes, a revision of CIGG's Term of Reference (ToR), Training of staff and IG key roles
- 32 were in progress and still within the revised timescales (52%),
- 2 elements not likely to be completed within timescales (3%), including the development of guidance over Members access to information,

- 3 were out of timescales (5%), which included the elements of a review of the current Data Protection Impact Assessment Template, review of the Regulations of Investigatory Powers Policy (although the revised Policy was approved by EMT on 8th August 2022 and was approved the relevant portfolio holder/ Cabinet in September 2022), the development of and implementation of an Information Request automated workflow app, and the creation of an exercising of data protection rights policy for the public.

3.3 Three CIGG meetings have taken place in the year where the implementation of elements of the plan are considered, and challenged where timescales have not been met, and areas of concern discussed, with actions required identified. These meetings are chaired by the Senior Information Risk Owner (SIRO), and take place quarterly, in line with the group's ToR.

3.4 Additionally, regular Corporate Information Operational Group Governance (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.

3.5 CIOG meet every 6 weeks, and 8 meetings have taken place through the year.

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. The Council's response to this enforcement order is via mandatory Cyber Security and GDPR training on an annual basis.

4.2 In April 2021 the compliance reporting for this training was automated to improve the provision of compliance data directly to managers within dashboards, alongside other mandatory training reports, thus assisting their management of their staff's training compliance.

4.3 Compliance details (Departmental breakdowns at Appendix 1)

	2nd April 20	1st April 21	31st March 22	1st April 22
Number of staff requiring training	2,391	3015	3254	3208
Number of staff trained	1,812	2314	2374	2369
Compliance rate	75.78%	76.7%	73%	74%
Number of Members requiring training				84
Number of Members trained				66
Compliance rate				78.6%
Target Compliance rate	95%			

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

4.4 A number of services who have higher levels of staff who do not use computers, at least not on a regular basis as part of their role, are following other avenues of undertaking this training, such as manual workbooks, small meetings etc. Their compliance rates are being monitored, by the CIGG in addition to their Head of Service who have access to the training data through the dashboards.

4.5 A Cyber Security and GDPR training course specifically created for Council members has been made available from May 2022 coinciding with the election of many new Council members and formation of the new Council and Cabinet.

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.

	2020/2021	2021/2022
Numbers of reported incidents	220	263
Number of personal data breaches	115	149*
Number of incidents reported to the ICO	7	11
Number of notifications to data subjects	5	0
Number of separate complaints made to the ICO over personal data breaches	3	4
Number of DPA breaches occurring externally	70	90
Number of DPA breaches occurring internally	44	57
Number of DPA breaches involving sensitive personal data	20	43
Number of DPA breaches contained	89	126

* 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 incident types is provided at Appendix 2.

5.4 There has been an increase of 19% in the numbers of information security incidents reported and of those incidents an increase in personal data breaches of 29%.

5.5 There has been an increase of 4 personal data breaches reported to the ICO, and an increase by 1 of complaints received directly from the ICO.

5.6 An analysis of incidents reported do not show any particular reason for the increases.

5.7 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. A training resource has been developed on how to investigate personal data breaches, since these are undertaken by the services, with support from the Information Compliance Team.

5.8 Those personal data breaches reported to the ICO include a misdirected grievance pack, publication of information on the web, data handling, recording, and accessing issues, and the unauthorised disclosure of information.

5.9 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.

5.10 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.

5.11 It was agreed during the year that these recommendations would form part of the Council's Regulatory Tracker, entries are now ready for approval from the SIRO, and upload for Qtr. 1 22/23

5.12 The ICO has provided 33 recommendations, within their decision notices. At this time, 23 have been implemented, and 10 are in progress of implementation. The implementation of recommendations may also be part of wider pieces of IMAG planned activities.

5.13 Some recommendations are repeated through different ICO decisions.

5.14 The four complaints made directly to the ICO relate to disclosure of information, information handling practices, and transparency of processing. In three of the four cases a breach of personal data had occurred. Where the Council was found to have breached personal data then two recommendations for improvements were made.

5.15 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 data

protection legislation, or affecting the integrity and availability of important information assets.

5.16 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 1109 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 1000 last year, an increase of 11%

6.2 The Information Commissioner has previously indicated that there is an expectation of a 90% compliance rate.

Information Regime	Numbers received	Compliance rate	Compliance up or down (percentage points)
FOI	788	84%	-4%
EIR	232	90%	-4%
SAR	89	63%	+6%
Overall	1109	83%	-2%

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

- 89% of non-compliant responses were due to delays by the service areas.
- 8% of non-compliant responses were 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.
- 3% of non-compliance was due to other factors.

6.4 Based on the data in paragraph 6.3 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 98%.

6.5 Reports detailing reasons for lateness, are supplied to CIGG.

6.6 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, covering many years, which have to be prepared, examined, and considered for disclosure, and redacting information, where deemed not appropriate for disclosure or not the personal data of the requester.

6.7 During the year the team have not only actioned more SARs, and improved the disclosure compliance rate, but have also reduced the number

of out of timescale SARs outstanding, figures below show those outstanding at as of 16th May 2022.

Year	Number O/S	Comments
2018	1	Being undertaken in batches and the DPO is in communication with requestor.
2019	0	
2020	1	
2021	6	

6.8 The deterioration in compliance rates for FOI and EIR requests can be attributed to

- Increased number of information requests over the three regimes
- Reduction in the numbers of Information Compliance Officers in the year
- Increased number of instances where delays were experienced in obtaining information to enable a response to the FOI /EIR request to be issued.
- Concerted efforts to reduce the number of historical SARs outstanding

6.9 Details of complaints over information requests

Complaint to Powys County Council – internal review	**17 (↓6)**	**Complaint made directly to the ICO**	**3 (↑1)**
Over lateness	1		2
General disagreement with response	13		1
Application of exemption	3		
Outcome – complaint not upheld	7		
Outcome – complaint upheld	0		3
Outcome – complaint partially upheld	7		
Still under consideration at 31-03-21	3		
Still under consideration from previous years	1 (2019)		

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 now comprises of 3 Information Compliance Officers, 1 Information Compliance Manager, 1 Assistant Data Protection Officer, and 1 Professional Lead Data Protection.

7.3 During the year a review of the team was implemented, taking account of the responsibilities, and required knowledge and skills of the staff, providing development opportunities and succession planning, in addition to releasing expected savings from the development of an automated workflow App, which has not yet been implemented. The number of Information Compliance Officers reduced from 5 to 3, but with an increase of grade commensurate with job description, and the implementation of the Assistant DPO post and deletion of the DPO school's post.

7.4 Due to this review the Professional Lead Data Protection now undertakes both DPO and IG activities, and is also the designated DPO for Schools, in addition to the roles of Regulation of Investigatory Powers Act 2000 (RIPA) Co-ordinator, and Senior Responsible Officer for Camera Surveillance.

8. Data Protection Officer

8.1 All public authorities, including each school as a public authority in its own right, are required to have in place a designated Data Protection Officer whose position and tasks are detailed within legislation.

8.2 In addition to the provision of advice and support, the DPO undertakes its monitoring responsibilities through reporting processes, and whilst working closely with service areas providing advice & support, managing the mandatory assessment of data protection risks for new ways of working, clear desk audits, compensation analysis or projects (Data Protection Impact Assessment), SWAP Audit reports, 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, due to the level of seriousness undertakes the necessary investigations.

8.4 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 and the Welsh Government's Homes for Ukrainians service, and the Council's wider response to these issues, such as information sharing agreements, analysis and development of dataflows, and Data Protection Impact Assessments etc

8.5 A separate annual report is developed for Schools.

9. Cyber Security

9.1 The Cyber Team consists of 2 members of staff who provide the service solely for the Council, until October 2021 this was a role which was split across the council and the Health Board but due to increasing workloads

and demands on the Cyber Security Service additional resource has been sought within the Health board to cover that role. Cyber security is no longer part of the Section 33 agreement.

9.2 In January 2022 the Council achieved Cyber Essentials Plus and IASME Gold accreditations for the 3rd year running. It is intended that the council will continue to maintain the standard and seek accreditation annually.

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. 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.

9.4 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 shift to homeworking for the majority of staff was achieved due to previous planning to enable sufficient and secure remote working practices. Additional Security was added to end user devices to enable them benefit from using their home broadband and still achieving the same level of Security protection as they would when connected to the Corporate network. A shift towards Zero Trust networking and Secure Access Service Edge (SASE) technologies is emerging as the council moved more to adopting Cloud technologies and Software as a Service. Additional Security tooling and software has also been adopted to further enhance and improve their Cyber Resilience as a result of capital investment into Cyber Security.

9.6 Additional Staff awareness and training specifically in detecting and reporting Phishing Emails has been undertaken towards the end of 2021 beginning of 2022, the outcome of which indicates that we still have further improvement required in this area.

9.7 The Cyber Security Manager continues to work on improving and reviewing Cyber Incident Response plans and with Senior Leadership Team involvement has undertaken a Cyber Incident Response exercise in March 2022. This was achieved using Welsh Government funding in Cyber Resilience in order to collaborate with an external organisation to deliver and facilitate the exercise. The Cyber Response plan continues to be developed and will be a key part of the Cyber Resilience Strategy.

9.8 Cyber Resilience reports are prepared quarterly for the attention of the Executive Management team, highlighting achievements, plans, issues and risks over the previous quarter.

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 employ individual DPOs.

10.2 The Head of Schools Services is provided with an annual DPO for Schools report, in line with the school year. The 2020-2021 report having been issued in January 2022.

10.3 Advice and support provided has been in relation to actioning SARs, and other data protection rights, with DPIAs being undertaken on Apps used by schools, and the use of data intermediaries, and appropriate agreements being developed to support the sharing of personal data. Monitoring responsibilities are delivered through working with individual schools. In addition to the management and undertaking of investigations where necessary, in particular those relating to a number of cyber incidents which occurred through a number of high schools.

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

11. Information Management Service

11.1 Service delivery on site for Information Management has continued uninterrupted throughout the pandemic. 406 file requests have been completed and returned to services in 2021/22. These have been sent in the main in hardcopy, but some smaller files have been scanned and sent electronically to staff who are homeworking.

11.2 Hard copy file collections have also resumed with staff collecting 251 boxes from around the county.

11.3 12,595 hard copy files have been destroyed in accordance with the corporate retention schedule.

11.4 The service level agreement with Powys Teaching Health Board continues and 849 file requests were received in 2021/22, and 7,888 boxes of records in total are now stored and managed by Information Management on behalf of Powys Teaching Health Board.

11.5 Staffing levels within the service have continued to be problematic with recruitment of professional staff challenging. Powys Archives and Information Management operate a fully integrated staffing structure, and service delivery of the archive service has also been affected. Further attempts will be made to recruit an Archives Manager and Archives Officer in 2022.

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 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.

12.4 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.

12.5 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 and resources to ensure effective governance but plans for future improvement are in place and are monitored by CIGG.

13. Planned Activity 2022-2023

- Continue with the development of information requests automated workflow processes and reporting, including chasing and recording of non-compliance rates and reasons. To include the provision of information directly to management dashboards, public reporting of compliance rates, and disclosures logs. Supported by a revised publication scheme and web pages.
- Continue to monitor training compliance rates.
- Continued implementation of IMAG plan, in particular developing funding applications to enable undertake reviews of Information Asset Registers, and so build into the Council's Record of processing activities and management of information.
- Continue close working relationships with cyber security staff, to ensure both technical security standards and information governance issues are addressed in tandem.

14. Resource Implications

14.1 The Deputy Head of Finance acknowledges the report and confirms there are no financial implications.

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

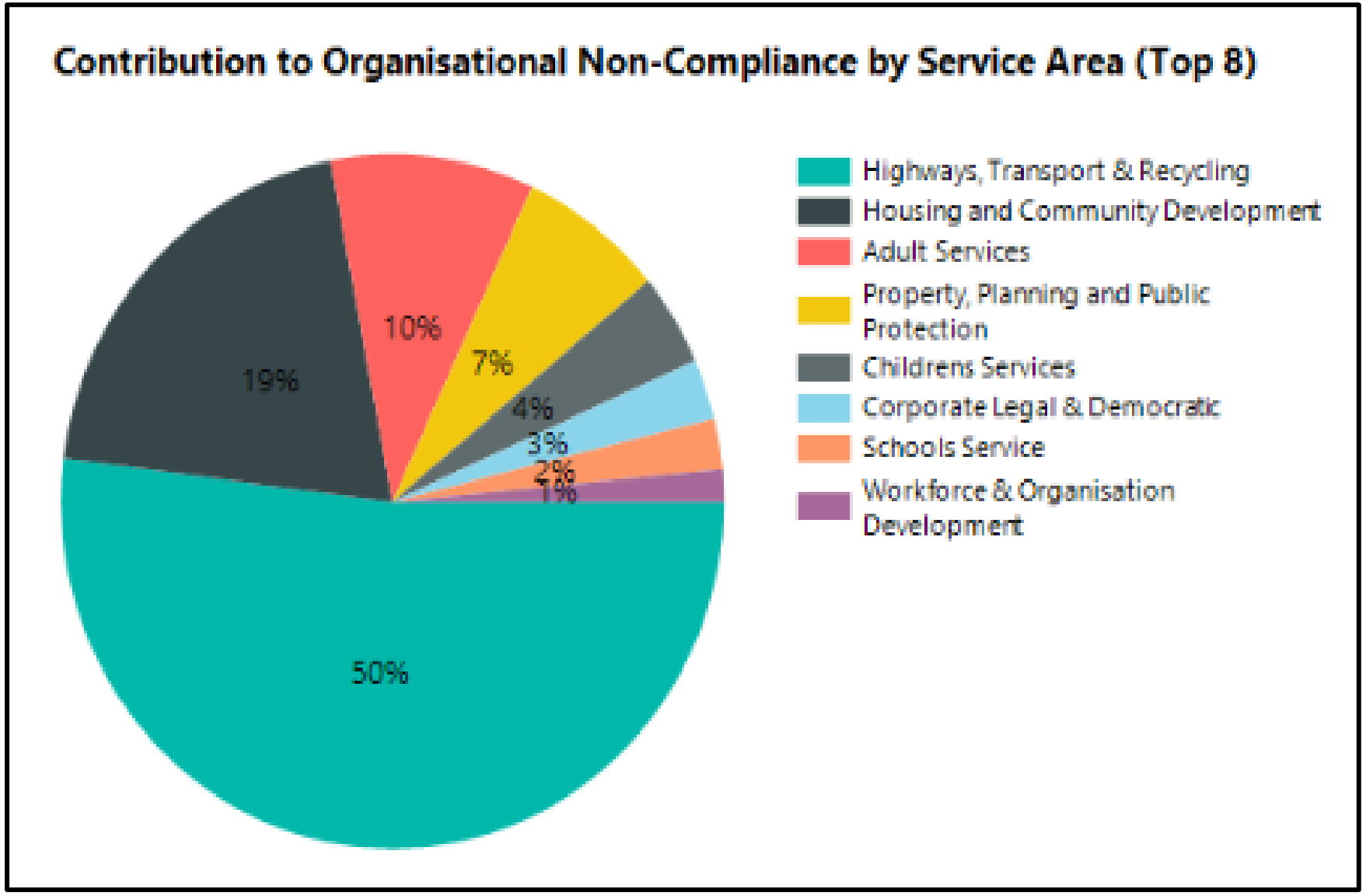
19. Recommendation

19.1 Cabinet notes the assurance set out in 12.5 and the planned activity for 2022-2023 as set out in paragraph 13.

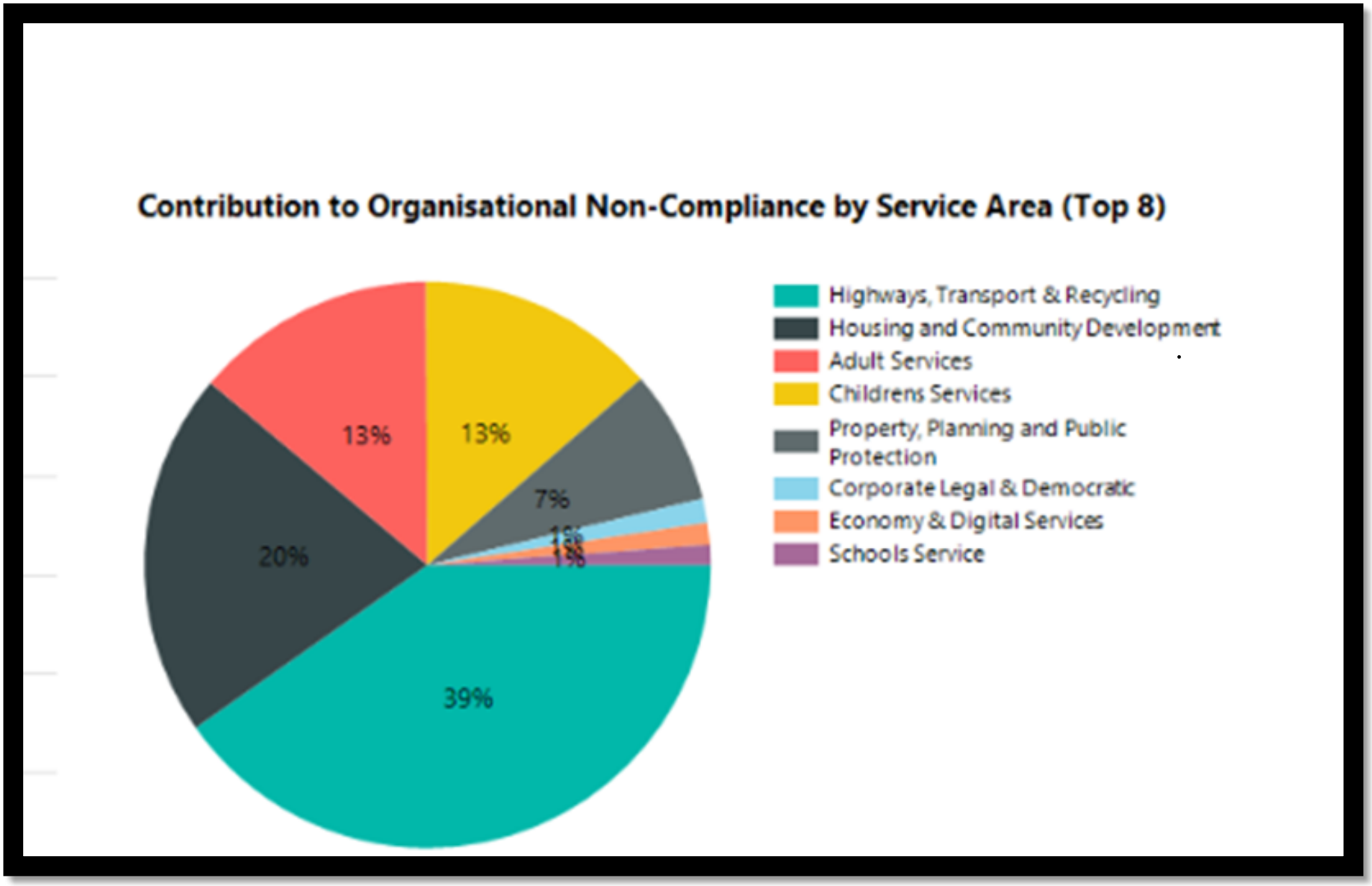
Contact Officer:	Helen Dolman
Tel:	015697 826400
Email: helen.dolman@powys.gov.uk	
Head of Service: Diane Reynolds	
Corporate Director:	Emma Palmer

Appendix 1

Cyber Security and GDPR Training April 2021 - noncompliance



Cyber Security and GDPR Training March 2022 - noncompliance



Appendix 2

Information security incident breakdown

Service Area	Numbers of incidents
Adult Services	34
Childrens Services	76
Commissioning	4
Digital Services	14
Finance	26
Housing & Community Development	15
HTR	7
Legal and Democratic services	9
Other	7
Property, Planning and Public Protection	24
Schools Services	21
Transformation and Communications	3
Workforce & organisational Development	23

Type of Incident	Numbers
Complaint	16
Cyber factor	5
Inappropriate access	10
Inappropriate processing of data	14
Information rights	25
Integrity of information	10
Loss of information	9
Loss/theft of equipment	1
Other	6
Physical Security	4
Unauthorised disclosure (External)	106
Unauthorised disclosure (Internal)	57