CYNGOR SIR *POWYS* COUNTY COUNCIL.

CABINET EXECUTIVE
Date: 21st May 2024

REPORT AUTHOR:	**County Councillor Jake Berriman, Cabinet Member for a Connected Powys.**
REPORT TITLE:	**Annual Information Governance Report 2022-2023.**
REPORT FOR:	**Information.**

1. Purpose.

1.1 To brief Cabinet on the on the Information Governance activities undertaken, and compliance achieved for the financial year 2022/2023, and to provide a level of assurance to Cabinet as to the Council's Information Governance arrangements and practices.

2. Summary.

2.1 Work has continued in the delivery of the Council's Information Governance activities, the core elements being:

- Monitoring of Cyber Security and General Data Protection Regulations (GDPR) training: Staff training compliance figures improved, Members' compliance figures declined. (See section 6)
- Management of personal data breaches reported; there was a slight increase in in the numbers of incidents reported, but a decrease in the number of those identified as breaches needing to be reported to the Information Commissioner (See section 7)
- Responding to the Council's formal information requests; there was a slight decrease in the numbers of requests received, and a slight decrease in response compliance rates. (See Section 8)

3. Background.

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

3.2 The Corporate Information Governance Group is responsible for providing advice and assurance to the Council on its Information Management, Assurance and Governance, and effectively manages the information governance framework.

3.3 The Head of Legal and the Monitoring Officer is the council's Senior Information Risk Owner and has delegated responsibility for information risks.

4. Information Management Assurance and Governance Plan.

4.1 The 2021-2023 Information Management Assurance and Governance plan was agreed by the Corporate Information Governance Group in March 2021.

4.2 As of the 31st of March 2023 there were 61 elements to the plan,

- Thirty-one had been completed (51%), such as:
  - the implementation of a revised publication scheme, and revised web pages, which explains to the public what information is available from the Council.
  - A Cyber Security Incident response exercise being undertaken.
  - Publication of a policy over the Council's use of special category personal data.
  - Revision of the Council's policy on Regulation of Investigatory Powers.
- Twenty-three elements were in progress and still within the revised timescales as approved by Corporate Information Governance Group (38%),
- Seven were out of timescales (11%), which included:
  - the development of guidance for Members on accessing information,
  - a review of postal checking regimes,
  - the development of a policy over the Council's installations and use of surveillance cameras,

4.2.1 Of those seven,
1 was ranked as being a high-risk element.
4 as medium risk elements.
2 as low risk elements.

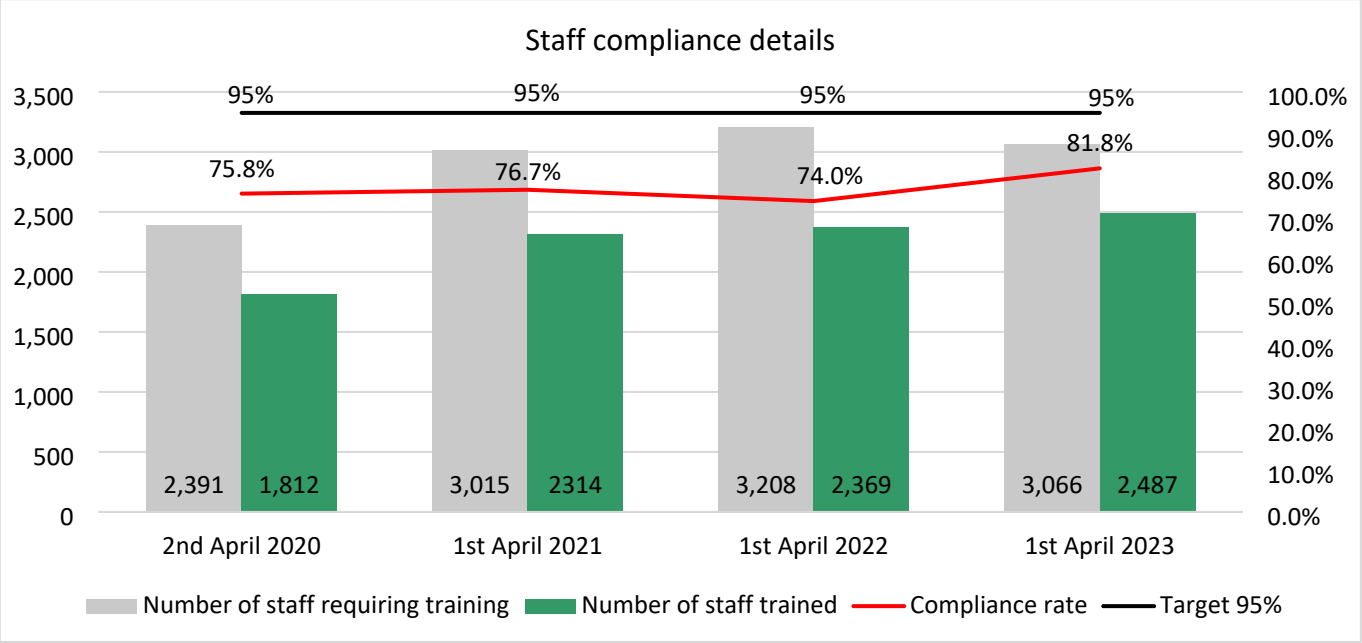
5. Oversight.

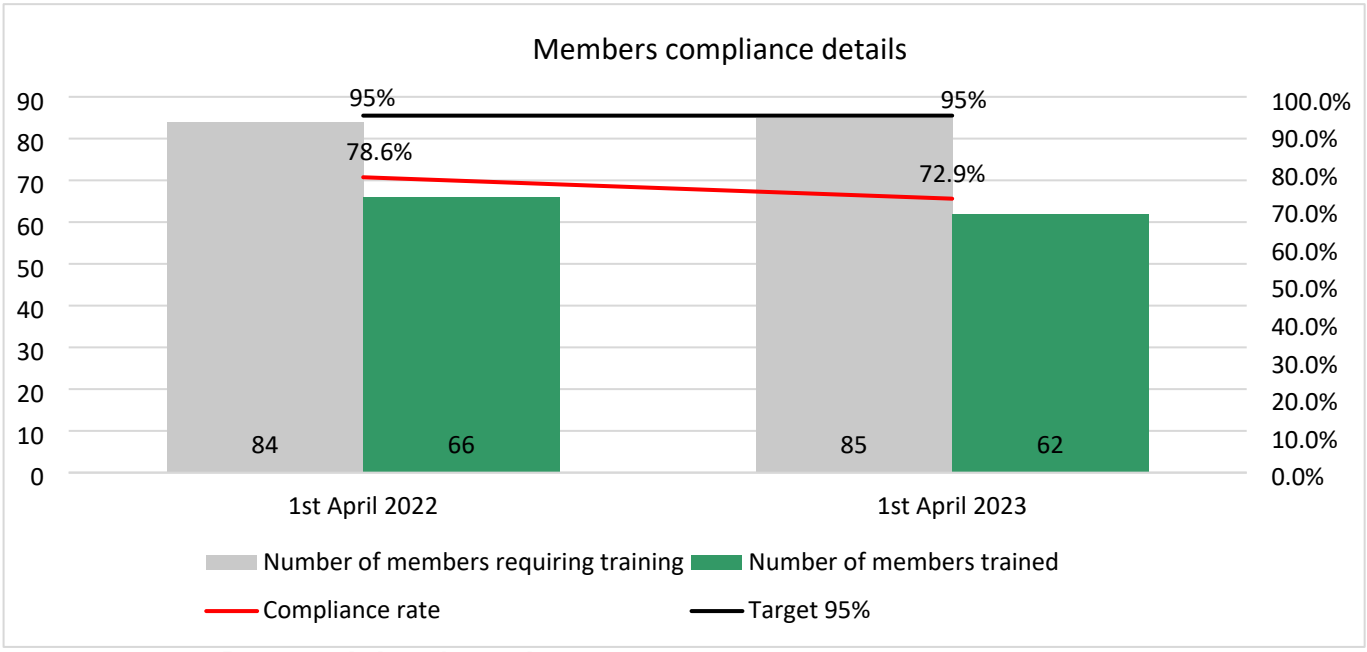
5.1 Three Corporate Information Governance Group meetings have taken place in the year. These meetings are chaired by the Senior Information Risk Owner and normally take place quarterly.

5.2 Additionally, 7 Corporate Information Operational Group Governance meetings have taken place, involving representatives of the Information Asset Owners, to discuss and monitor Information Governance matters and measurements and to carry out work activities as directed by the Corporate Information Governance Group. These meetings take place every 6 weeks.

6. Cyber Security and GDPR mandatory training.

6.2 Compliance details (See departmental breakdown at Appendix 1)

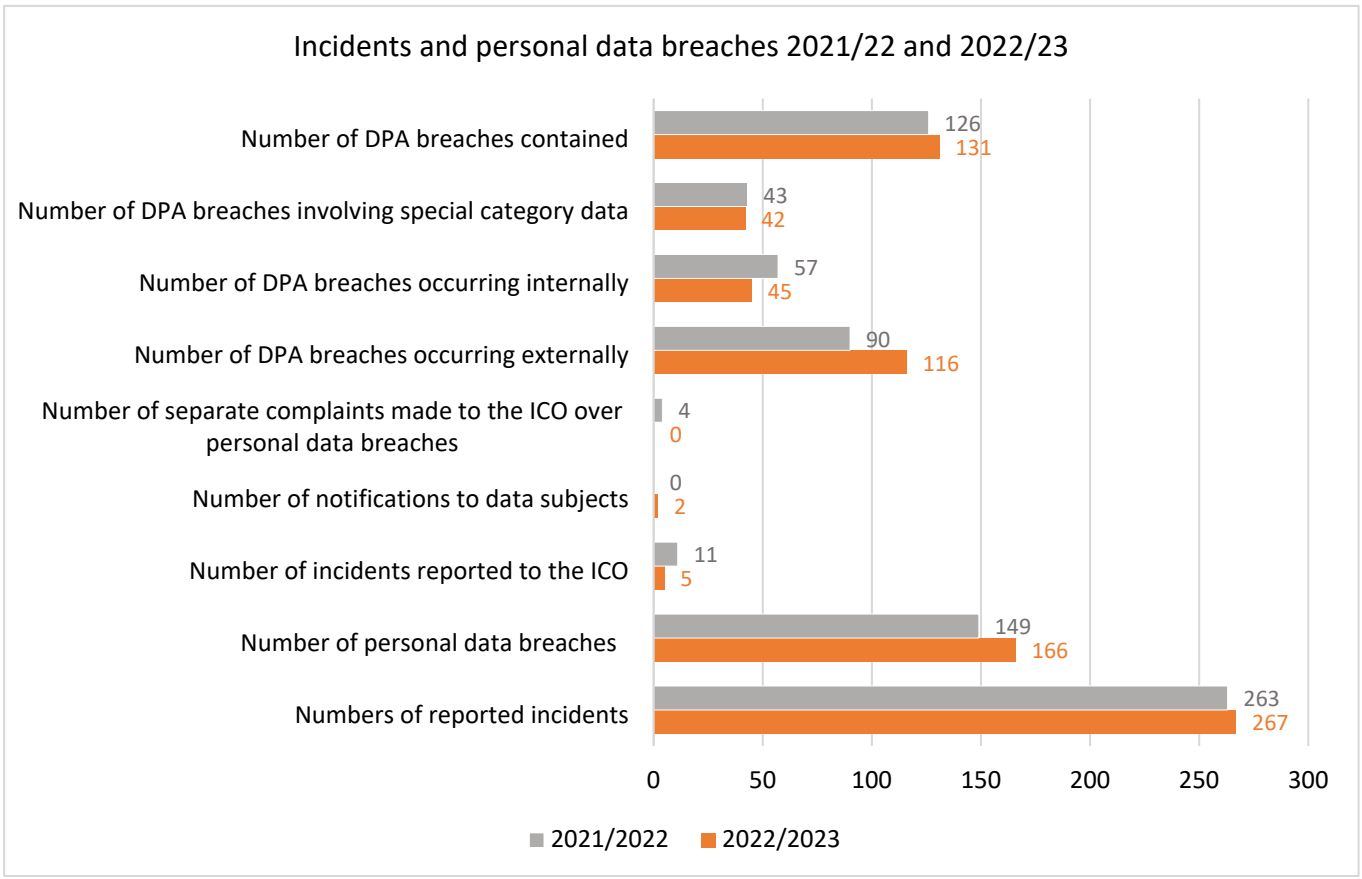




7. Personal data breaches

7.1 Given the amount of personal data service areas handle it is realistic to acknowledge that human errors will occur and may result in a personal data breach. The Council has robust reporting and management processes in place, which continue to ensure swift containment action, informed identification of information risks and mitigation, and supports relevant reporting obligations, to both the regulator and data subjects.

7.2 Figure 7.2 below provides details of incidents and personal data breaches, and comparison data from last year.



* using the definition of a personal data breach within the UKGDPR. 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.

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

7.4 There has been a 1.5% increase in the numbers of information security incidents reported but an increase of 11% of those identified as a personal data breach. However there has been a decrease of personal data breaches reported to the ICO, due to the breaches having occurred resulting in less risk to the individual, and no complaints having been received directly from the Information Commissioner.

7.5 Analysis of reported incidents indicate that the following account for the highest number of reported incidents:

- misdirected emails.
- disclosure of information through postage,
- attachment of incorrect documentation to emails
- verbal disclosure,
- printer issues,
- incorrect redactions

7.6 Misdirected emails have been reported separately as the Information Commissioner refers to these within their annual report on data security

trends as the reason behind most incidents reported to them. Taking account of the differences in reporting, then Powys County Council reflects similar trends, to those seen nationally.

7.7 Whilst the majority of incidents can be attributed to human error, it is not always possible to establish why these errors occurred. Where training or processes are found to be lacking then recommendations to prevent similar occurrences are discussed with the service.

7.8 Those five personal data breaches reported to the Information Commissioner include:

- paperwork for one party being left in the home of another,
- scanned documents not being received by service area,
- information sent to the wrong address,
- publication of personal data on the web,
- cyber incident affecting a supplier.

7.9 Of the five, two remain outstanding with the Information Commissioner, awaiting a decision. But in three cases the Information Commissioner has found that the Council breached data protection legislation.

7.10 Whilst no regulatory action, such as fines or enforcement orders, has been taken the council, where the Information Commissioner has recommended further activity to improve, then these recommendations are reported and on the Regulatory Tracker and implemented by the relevant service area or organisation as appropriate.

7.11 During the year the Information Commissioner has provided 24 recommendations within their decision notices. Twenty-two have been implemented, and 3 are still in progress, with 3 recommendations still open from previous years and will form part of wider pieces of Information Management Assurance and Governance planned activities.

7.12 Of those recommendations outstanding

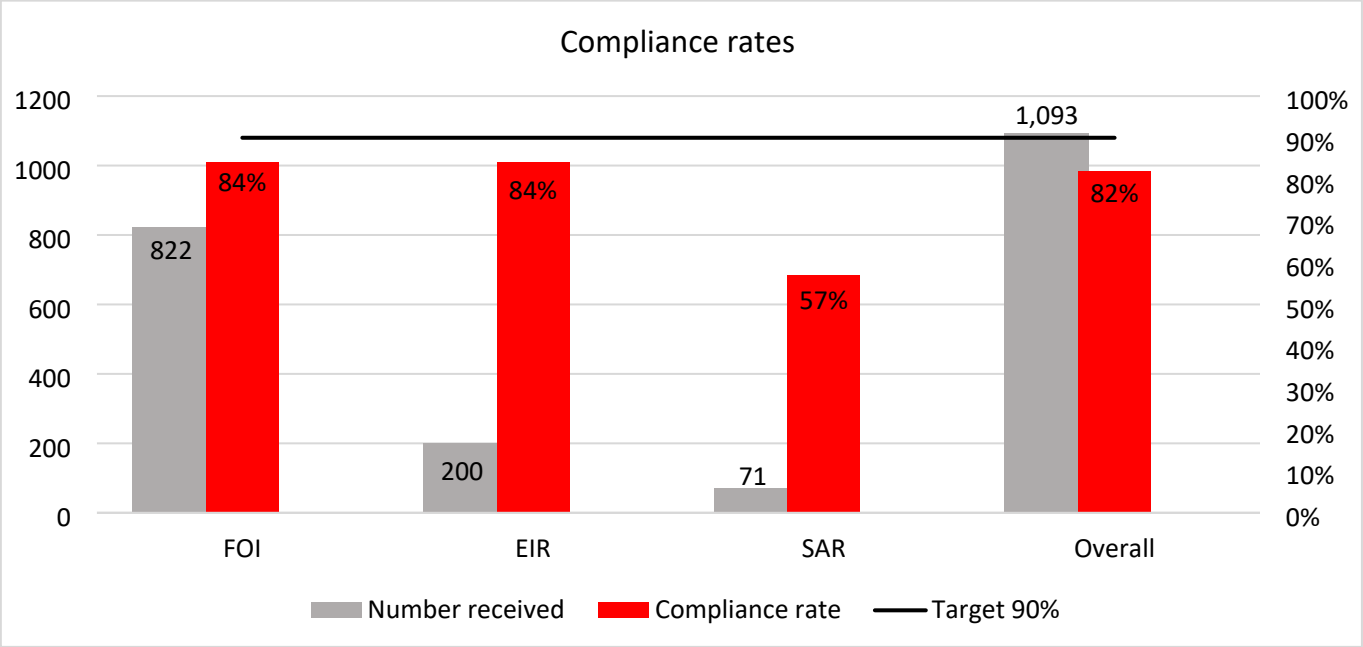
- 2 relate to the implementation of naming conventions for documents. New Management of Electronic Information Officer post with include within their forward work programme.
- 1 relates to the use of autosave within Office 365 products. New Management of Electronic Information Officer post with include within their forward work programme.
- 2 relate to checking regimes when sending personal data outside of the organisation. Review of postal checking regimes has commenced.
- 1 relates to the use of appropriate security and postal measures dependent upon content of the envelope. Guidance being developed for services.

8. Information Requests

8.1 There were 1093 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, compared with 1109 last year, a decrease of 1.4%

8.2 The Information Commissioner has previously indicated that there is an expectation of a 90% compliance rate in responding to information requests, within legislative timescales.



8.3 In comparison with the previous year (21/22) the compliance rates are as follows:

- FOI same compliance rate.
- EIR down by 6 percentage points.
- SAR down by 6 percentage points.
- Overall, down by 1 percentage point.

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

- 92% of non-compliant responses were due to delays by the service areas providing information to enable a response to be drafted.
- 5% 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, such as IT issues or lack of agreement how to proceed with the request.

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

- Increased number of instances where delays were experienced in obtaining information from services.
- Efforts taken to ensure the number of SARs outstanding are managed even if not responded to within timescales and that backlogs don't build.

8.6 Details of complaints received over information requests.

Complaint to Powys County Council– internal review	**36** (↑19)	**Complaint made to the ICO**	**11** (↑8)
Over lateness	3		7
General disagreement with response	29		4
Handling of request	4		
Outcome – complaint not upheld	16		4**
Outcome – complaint upheld	17		7
Still under consideration at 31-03-21	3		

8.7 The Information Commissioner has subsequently found in favour of the Council's position on the 4** complaints not upheld.

8.8 The Information Compliance Team also deliver a Data Protection Officer and Information Governance support for each of the Schools in Powys, rather than them each having to employ individual Data Protection Officers.

9. Information Management

9.1 The council's inactive hard copy records continue to be manged by the Information Management Unit.

9.2 Further to risks being identified over the management of the council's electronic information then funding was approved to enable the introduction of a specific post to mitigate and manage some of these risks.

10. Conclusion

10.1 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 and safely is essential.

10.2 The work being undertaken towards compliance with data protection legislation and other information legislative regimes must continue, in order to reduce information risk, and the likelihood of regulatory action. A mature information governance framework will support the Council's transformational portfolio and its ambition of being stronger, fairer, greener.

10.3 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 the Corporate Information Governance Group.

11. Planned Activity 2023-2024

- Recruitment of additional Information Compliance Officer to concentrate initially on SAR, and a Management of Electronic Information Officer to review work already undertaken on Information Asset Registers, and develop polices, and procedures to ensure the appropriate management of council information.
- Continue to develop the knowledge and skills of the Information Compliance team to be able to address any number of different Information Governance issues.
- Monitor the likely impact of the Data Protection and Digital Information Bill.
- Develop an Information Management Assurance and Governance plan 23-25.

12. Resource Implications

12.1 The Information Governance function is delivered in the main through the Information Compliance team, with a budget allocation of £210,070, with £80,000 being provided from Schools Service for the delivery of a Data Protection Officer service to all schools. Activity at service level is undertaken within existing budgets.

12.2 The Head of Finance (Section 151 Officer) notes the report.

13. Legal implications

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

13.2 The Head of Legal and the Monitoring Officer notes the legal comment and supports the recommendation.

14. Data Protection

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

15. Climate Change & Nature Implications

15.1 The report has no climate change nor nature implications.

16. Comment from local member(s)

16.1 NA

17. Integrated Impact Assessment

17.1 NA

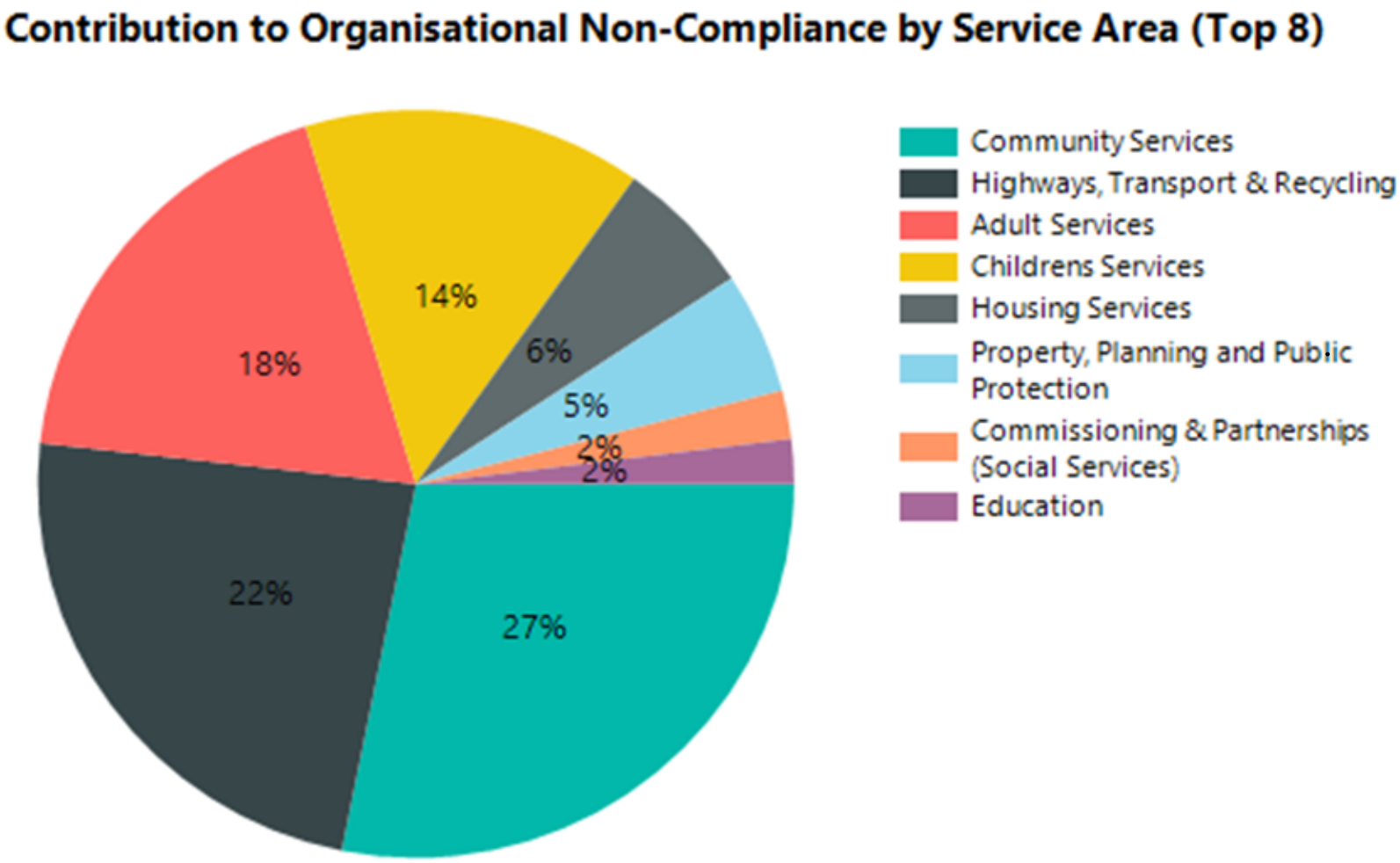
18. Recommendation

18.1 Cabinet notes the assurance set out in 10.3 and the planned activity for 2023-2024 as set out in paragraph 11.

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

Appendix 1

Cyber Security and GDPR Training April 2023 - noncompliance



Appendix 2

Information security incident breakdown

Service Area	Numbers of incidents
Adult Services	41
Childrens Services	84
Commissioning	5
Digital Services	13
Finance	17
Housing & Community Development	9
HTR	5
Legal and Democratic services	9
Other	15
Property, Planning and Public Protection	16
Schools Services	22
Transformation and Communications	3
Workforce & organisational Development	28

Type of Incident	Numbers
Unauthorised disclosure	85
Misdirected external email	73
Misdirected internal email	34
Complaint	17
Cyber factor	5
Inappropriate access	11
Inappropriate processing of data	8
Information rights	11
Integrity of information	5
Loss of information	13
Other	4
Physical Security	1