Appendix 1

2022/23 Annual Report

Senior Information Risk Owner (SIRO)

Information Governance - assurance and performance.

Jan 2023

Presented to Audit & Assurance Committee 9 March 2023

Contents

Executive Summary

This report provides an update relating to the responsibilities of the Cumbria County Council Senior Information Risk Owner (SIRO) and outlines activity and performance related to information governance for the period 1 April 2022 to 31 December 2022. The report provides assurances that information risks have been effectively managed and where improvements have been implemented.

The County Council continues to be committed to effective information governance, with robust arrangements in place to ensure the council complies with legislation and adopts best practice. Governance arrangements are closely monitored to ensure systems, policies and procedures are fit for purpose, accommodate new working procedures and that all staff and elected members understand the importance of information governance and security so that good practice is everyone's business and embedded as part of the Council's culture.

ICT security and cyber risks continue to present an increasing global, national and local challenge to all organisations and the Council is no different. Arrangements to manage these risks are contained in the report with a summary included to list action already undertaken to maintain and strengthen defences and enhance corporate resilience.

A summary of the key achievements and issues in the past year include:

- Successful compliance with the requirements for ongoing access to the national Public Service Network (PSN).
- Successful completion of the NHS requirement for an annual submission to be provided by the authority to show compliance with their Data Security & Protection Toolkit.
- Slight decrease in performance in handling data subject access requests where 83% of cases were responded within one calendar month in 2022/23 compared with 86% in 2021/22. However, this performance should be taken in the context of managing a 33% increase in requests received when comparing with the previous year.
- Performance in handling Freedom of Information / Environmental Information Requests remains static at 84% in 2022/23 when comparing with requests responded to within 20 working days the previous year.
- The GDPR phase 2 internal audit follow up audit concluded the maximum 'reasonable' audit assurance opinion in July 2022.
- The ICO Data Protection Accountability Assessment has been updated. The assessment includes 340 questions across 10 thematic areas.
- The Legal and Democratic Services (Data Assurance Working Group) has focused on delivery of the Data Assurance Delivery Plan, which includes the minimum legal requirements that both new Unitary Councils of Cumberland and Westmorland & Furness have in place in the run up to and beyond 1 April 2023 Vesting Day. The Group has successfully progressed a number of core areas:
  - Understanding and clarifying registration requirements.
  - Systems required to manage Data Protection Impact Assessments/Data Sharing Agreements and Privacy Notices.
  - Governance and processes for handling data breaches and security incidents.
  - Employee training and communications.
  - Ratification of Record Retention and Disposal Schedules and associated guidance.

Introduction

1. This Senior Information Risk Owner (SIRO) Annual Report reflects on the Council's information governance work undertaken from April 2022 to December 2022 so that a report can be provided to the County Council Audit & Assurance Committee before the Council ends on 31 March 2023. The report provides assurances that personal data is held securely, information is disseminated effectively and provides an overview of key performance indicators relating to the Council's processing of information requests within the necessary legal frameworks.

2. Specifically, this report:

   a) Provides assurance as to the work undertaken and on-going in relation to Cumbria Local Government Reform and the actions taken by Cumbria County Council in advance of the 1st April 2023 Vesting Day.

   b) Documents organisational compliance with the legislative and regulatory requirements relating to the handling and processing of information and provides assurance of ongoing improvement to manage information risks. This includes the Councils consideration and performance relating to:

      - UK General Data Protection Regulation (UK GDPR)
      - Freedom of Information Act (2000)
      - Environmental Information Regulations (2004)
      - Information Security Standard ISO/IEC 27002:2007
      - NHS Information Governance- Data Security & Protection (DS&P) Toolkit.

   c) Summarises any data breaches within the preceding nine months, relating to any risk relating to personal data loss or breaches of confidentiality.

Key Roles and Responsibilities

3. The Assistant Director Organisational Change (Interim Director Corporate, Customer and Community Services) assumed the Council's Senior Information Risk Officer role on 25 June 2022 and was responsible for:
   - Leadership and overall ownership of the Council's Corporate Governance arrangements, acting as corporate champion for information governance.
   - Providing a focus for management of information governance at a senior level.
   - Providing advice and reports in respect of information incidents and risk.
   - Owning the management of information governance and risk assessment processes within the Council.
   - Understanding how the strategic priorities of the Council may be impacted by information governance risks, and how these risks need to be managed including the adequacy of resources and levels of independent scrutiny;

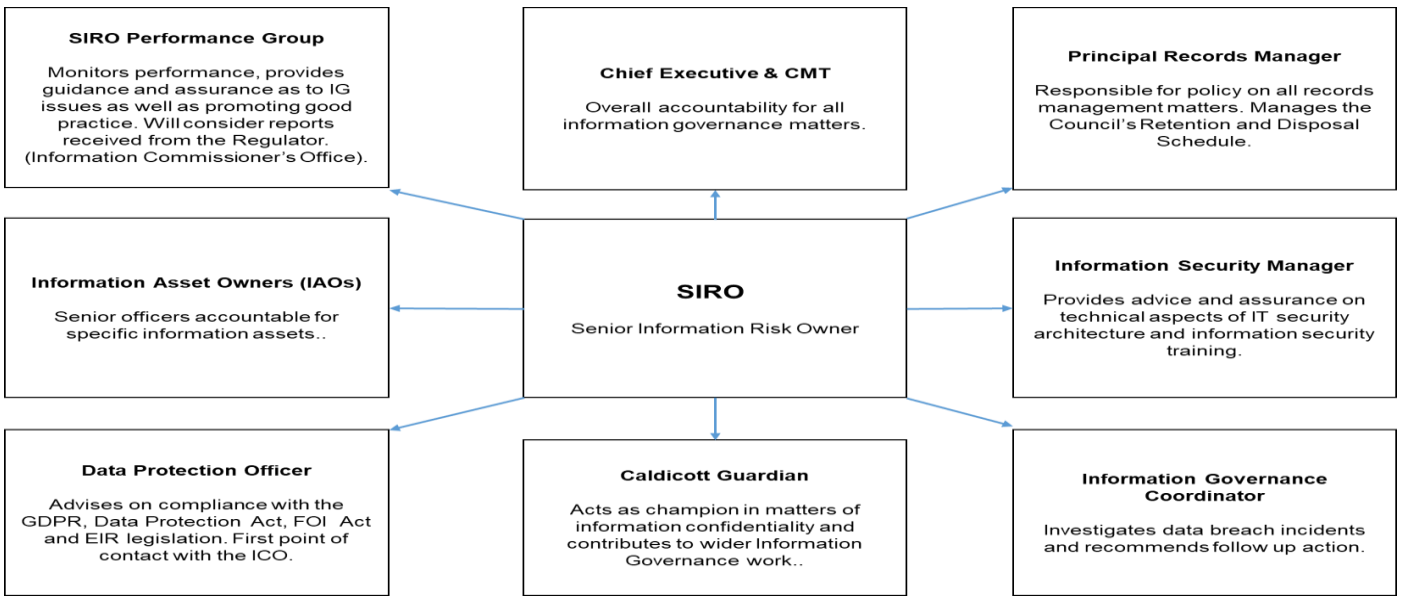
4. There are a number of officers and teams across the Council that have professional expertise relating to information governance and information security. It is however important that information governance must be everyone's business, with all staff and elected members having personal responsibility to ensure information and data is held securely, processed appropriately and safely destroyed when not required.

Governance and Monitoring Arrangements

5. The Council's SIRO is supported via the SIRO Performance Group which monitors Information Governance actions and performance and promotes information governance across the Organisation. More specifically the responsibilities of the SIRO Group is to:

- Support the SIRO to develop and improve the management of information governance.
- Promote and ensure awareness of applicable information governance policies and working practices and procedures for the effective use and protection of information assets.
- Provide assurance that capacity and capability is available to enable policies, procedures and processes to be developed and implemented.
- Provide assurance that the Council undertakes or commissions sufficient reporting, assessments and audits of information governance policies and operations so as to ensure that their implementation and practice both complies with the written policy and that the outcomes are measured to ensure intended benefits are delivered.
- Oversee Public Service Network (PSN) accreditation and implementation of and compliance with the NHS Data Security & Protection Toolkit.
- Support and promote the completion and maintenance of the Council's Information Asset Register. This will include providing oversight of the identification of information risks.
- Provide assurance that national developments in information governance policy and legislation are monitored and acted on.
- Ensure information governance incidents are appropriately and promptly investigated and reported.
- Monitor the Council's entry on the Register of Fee Payers for Data Protection purposes.
- Provide assurance that where there are changes in processes or working practices that appropriate information governance risk assessments or Data Protection Impact Assessments (PIAs) are undertaken.

The diagram below shows the SIRO relationships with officers across the Council.



Risk Management and Assurance

6. The Council's Corporate Risk Register for 2022/23 continued to include an Information Security risk, which is a combination of Data Protection and ICT Cyber Security threats. The main causal factors underpinning this risk align with the Key Principle of the UK GDPR, to implement effective technical and organisational measures to protect personal data. The risks are described as follows:

"There is a risk that the Council will experience a significant information security incident.

This may be caused by;

- *Inadequate technical information security arrangements.*
- *Inadequate organisational measures, including internal controls relating to policies, plans, asset registers, incident response and reporting arrangements, training awareness and ongoing learning.*
- *Inadequate surveillance camera arrangements.*

This may result in;

- *Disclosure of personal data leading to personal distress, damage and embarrassment as well as potential liability claims.*
- *A data breach leading to financial penalties & intervention by the ICO.*
- *A cyber incident leading to a partial or total interruption to service delivery to customers, suppliers or partners leading to partial or non-delivery of corporate priorities and having a reputational impact".*

7. As part of the Council's governance and assurance arrangements, a corporate strategic risk report is presented quarterly to Corporate Management Team, Cabinet Members and the Audit & Assurance Committee meeting to update on the effectiveness of risk management controls to manage or mitigate the risks. This report includes the Information Security Arrangements risk.

8. Throughout 2022/23 the Information Security Arrangements corporate risk has maintained a consistent risk rating of 15 (Impact of 5 x Likelihood 3). This is in line with the target risk score of 15 reflecting the scale of international cyber risk.

Ongoing ICT Cyber Security Threats

- International, national and regional cyber-attacks remain a high and ever-increasing threat to County Council ICT systems and the potential loss of personal information and data. The actual consequences of this type of incident would be significant to the continuity of Council Services and potentially serious impacts to council service users and employees.
- Knowing how significant the impact of an attack like this would be, the Council has over the last year continued to strengthen information security controls to minimise the likelihood of an external cyber-attack. Many of these security measures are regularly penetration tested as well as independently assessed with positive progress acknowledged.

Ongoing Data Protection Threat

- Ongoing communication campaigns and awareness raising alongside the mandatory completion of information security & data protection training continues to be monitored throughout the year.
- On investigation of the data breaches, the majority are the result of human error rather than a systemic or governance failure.

Corporate Governance actions

9. The Council is committed to a clear strategy and sustainable framework for information governance across the organisation. A SIRO Performance Group is in place to monitor performance reports, approve policy and procedures, review data breach trends and learning, consider Information Commissioner's Office (ICO) decision notices and to provide communications. The communications are designed to support learning and development of cultural behaviour to improve the Council's arrangements around data handling, processing and security.

10. The following key actions were delivered in 2022/23 which have strengthened the Council's management of information risks.

- Staff are required to complete mandatory Information Security & Data Protection training on an annual basis. A revised course for 2022 was launched in April, which includes lessons learned from data breaches that have been reported. Completion of the course remains mandatory for all staff with reports available for all managers to monitor completion of the course by their staff. At the end of December 2022 a performance rate of 79% had been achieved with 5141 CCC staff having completed the 2022 course. Regular reminders are issued to maximise completion against the 95% target.

- The NHS requires an annual submission by the County Council to show compliance with their Data Security & Protection Toolkit. For 2022/23, this was successfully submitted on 21 June 2022. Work is currently underway in preparing submissions for Cumberland Council and Westmorland & Furness Council.

- The County Council also needs to comply with the requirements for ongoing access to the national Public Service Network. (PSN). For 2022/23 this was achieved on 5 May 2022 which gave PSN compliance certification for 12 months.

- The County Council's ICT Security Manager is co-ordinating resources across all 7 sovereign councils involved in the Cumbria LGR programme to ensure appropriate ICT and cyber security arrangements are in place for the two new Unitary Councils from 1 April 2023.

- The County Council's Information Security Manager and Data Protection Officer have proactively worked with the LGR Theme leads, Technical Leads, Project Managers and Work Package Project Officers to ensure that core requirements are captured and that proposals are compliant with data protection legislation.

- Information Security Awareness month took place during November 2022 which included providing advice and answering questions on Information Security, Data Protection and Records Management. Activities included on-site visits across key County Council locations, on-line Question & Answer sessions and weekly communications.

Data Protection Assurance

11. **Part 1: Cumbria County Council.** To provide assurance in relation to the level of data protection compliance at Cumbria County Council in its final year of operation, the ICO Data Protection Accountability Assessment has been updated. The assessment includes 340 questions across 10 thematic areas:

- Leadership and Oversight.
- Policies and Procedures.
- Training and Awareness.
- Individuals' Rights.
- Transparency.
- Records of Processing Activities (ROPA) and Lawful Basis.
- Contracts and Data Sharing.
- Risks and Data Protection Impact Assessments (DPIAs).
- Records Management and Security.
- Breach Response and Monitoring.

12. The council has improved its data protection practices significantly since the General Data Protection Regulation (GDPR) came into force in May 2018. Noteworthy developments include:

- Governance arrangements.
- Policy framework.
- Employee training and communications.
- Data breach response and monitoring.

13. The outcome of the assessment applicable to the County Council resulted in 22 of the 340 Questions not being relevant for us, so for the remaining 318 Questions the compliance outcome was as follows:

Activity	**Outcome**	**%**
Fully Meeting ICO Expectations	314	98.74%
Partially Meeting ICO Expectations	3	0.94%
Not Meeting ICO Expectations	1	0.32%
Total	**318**	**100%**

14. The 3 areas where the council is only **'Partially Meeting Expectations'** are:

- Provision of regular training and certification for IG professionals.
- Periodic risk assessments of the council's Information Asset Register.
- Discussion of data protection/information governance KPIs at operational level.

15. Whilst all three areas have been actively discussed during 2022/23, progress has been affected by the diversion of resources to prepare for the implementation of Local Government Reorganisation in Cumbria on 1 April 2023.

16. The only area where the council is '**Not Meeting ICO Expectations'** is:

- the control of social media and messaging apps, including WhatsApp.

As the council recovers from the COVID 19 Pandemic and reverts to new ways of working, the ongoing use of social media and communication applications for council business is being constantly monitored with advice being requested from the council's SIRO and Information Security Manager regarding ongoing deployment and level of risk to the processing of personal data.

17. Overall, the outcome of the assessment is extremely positive and reflects the work done by a range of colleagues and teams across the council, to ensure that data protection is maximised. As we transition into two new unitary authorities, significant assurance can be given that the council has:

    - Taken steps to ensure its employees have a high level of awareness of security and data protection issues.
    - Ensured that tools, training and guidance have been made available to build a positive data protection culture.

18. **Part 2: Local Government Reorganisation (Cumbria) Programme.** Data protection has formed an intrinsic part of the LGR Programme from an early stage and data protection colleagues from all seven authorities have been actively involved in:

    - Data Protection Working Group
    - LGR Data and Intelligence Hub
    - Legal and Democratic Services – Data Assurance Working Group

19. Workload can clearly be divided into two distinct areas:

    - Provision of advice and guidance to the LGR Data and Intelligence Hub and wider LGR Programme
    - Delivery of the Legal and Democratic Services – Data Assurance Delivery Plan.

20. Support to the LGR Data and Intelligence Hub has focused primarily on the delivery of a Data Sharing Agreement and robust security and restricted access arrangements to cover the sharing and processing of data between the existing 7 sovereign councils as we prepare for the two new unitary authorities and new Fire & Rescue governance. These include key programme requirements such as Secure storage, Data Protection Impact Assessments and Privacy Notices to cover the transfer of employee data.

21. The Legal and Democratic Services - Data Assurance Working Group has focused on delivery of the Data Assurance Delivery Plan, this includes the minimum legal requirements that both new authorities have in place in the run up to and beyond Vesting Day. The Group has worked hard on a number of core areas:

    - Understanding/clarifying registration requirements.
    - Systems required to manage Data Protection Impact Assessments/Data Sharing Agreements and Privacy Notices.
    - Governance/process for handling data breaches/security incidents.
    - Employee training and communications.
    - Ratification of Record Retention and Disposal Schedules and associated guidance.

22. It became apparent via the review process that there are significant differences at County and Borough, City, District level in application of legal concepts and the tools available to manage them including variances in processes and procedures. There is also a difference in the level of involvement and oversight afforded to the Data Protection Officer in each authority and some interpretations relating to the obligations of the DPO and resources available across different ways of working.

23. To provide assurance of arrangements made for the safe transition from predecessor to successor authorities a number of actions have been taken:

- Identification of core compliance requirements for each new authority recorded and progressed via the Data Assurance Delivery Plan.
- Development of a Data Protection and Information Security Assessment to support delivery of the LGR Inter-Authority Agreement (IAA).
- A Memorandum of Understanding to cover the legal obligations of both new authorities in relation to services or systems not covered in detail by the LGR IAA.

Data Breach Management and Reporting

24. Any concerns relating to potential data breaches are promptly investigated and scored based on scale, assessment of numbers of people affected, sensitivity, nature of breach and likely impact. Dependent on the assessment score and discussion with the Council SIRO or Caldicott Guardian, the issue may be self-referred by the Council to the Information Commissioner's Office (ICO). The reporting, containment actions, investigation and learning phases of data breach incidents play a key role in the management of risk and improvement of internal controls.

25. All breaches and near misses are reported promptly to the Senior Information Risk Owner and discussed on at least a weekly basis. Consideration is given to whether the incident should be referred to the Information Commissioner's Office (ICO) within 72 hours. Following assessment by the SIRO Group, a total of three cases were referred to the ICO between April & December 2022, which is the same total amount reported in 2021/22. All three cases have been closed by the ICO without any further action or fines being applied. The ICO does however make recommendations as a result of any investigations they undertake as to what actions they expect to be taken by the Council to avoid re-occurrence.

26. During the period April – December 2022, the Council recorded and investigated 164 potential data breaches. The number of incidents reported provides evidence as to the awareness of the requirement to ensure data is held securely and processed in line with legislative requirements and to report incidents in a timely manner when a potential breach occurs. The category and numbers of each potential breach are outlined in the table of the following page.

Category of Potential Breach	No. recorded 2020/21	No. recorded 2021/22	No. recorded Apr – Dec 2022
Data posted or emailed to incorrect recipient.	130	123	99
Failure to redact data	2	7	2
Loss / Theft of mobile device	1	3	1
Loss / Theft of paperwork	2	0	10
Data left in insecure location	6	3	2
Verbal disclosure	6	2	5
Near miss / Non event	0	0	0
Unauthorised system access	8	6	2
Failure to use 'Bcc' option when sending an email	1	8	2
Information uploaded to webpage	5	2	4
Unlawful disclosure of sensitive / personal data	29	38	16
Other failure	6	8	8
Insecure disposal of paperwork	0	0	0
Others	8	17	13
Total	**204**	**217**	**164**

27. The breach assessment process includes a risk rating in relation to the incident as shown in the table below:

Risk Rating	No. recorded 20/21	No. recorded 21/22	No. recorded – Dec 2022
0- No Loss	**75** (37%)	**55** (25%)	**51** (31%)
1- Low Risk	**87** (43%)	**80** (37%)	**63** (38%)
2- Medium Risk	**41** (20%)	**79** (36%)	**47** (28%)
3- High Risk	**1** (1%)	**3** (1%)	**3** (2%)
Total Breaches	**204**	**217**	**164**

28. Significant focus is placed on learning from breaches and incidents of concern reported. As part of the investigation of an incident, learning actions are captured to identify opportunities to reduce the chances of a similar breach occurring in the future. This may see additional steps incorporated into a process before documents are issued, standard templates created to avoid the inclusion of incorrect information or post being issued via recorded delivery where appropriate.

29. Learning is shared across the organisation via the Information Security E-Learning training, corporate messages, targeted communications advising of incidents and through the Information Security week campaign.

Freedom of Information (FOI) & Environmental Information Regulations (EIR)

30. From April 2022 – November 2022 (the latest data available at the time of producing this report) the Council received 808 requests for information under the Freedom of Information Act and the Environmental Information Regulations.

Year	Requests Received	Processed on time	Performance (Target (90%)
2020/21	1209	1002	83%
2021/22	1112	932	84%
April – Nov. 2022	808	677	84%

31. The Council responded to 677 requests within the 20-working deadline required for responses. With a performance rate of 84% being achieved this remains in line with 2021/22 performance.

32. A Service Lead was recruited and has been in post since April 2022 to support and lead the development and day-to-day management of the Information Governance Team and further develop reporting and quality assurance of responses.

UK GDPR / Data Protection Act (2018)

33. Under the Data Protection Act 1998, any living person, regardless of their age, can request information about themselves that is held by the Council. This application process is referred to as a Data Subject Access Request (DSAR). In the last three years the council has handled the following requests.

	2020/21	2021/22	Apr – Nov 2022
Requests Received	224	225	197
No. actioned within 1 Month	151	188	164
% actioned within 1 Month	67%	86%	83%

34. The Information Governance Team based within the Service Centre receives and handles requests for data in relation to Children and People Management. Adult Social Care records are allocated to the appropriate service area for processing although this is supported by the IG team.

35. The performance level of responding within one calendar month at 83% shows a slight reduction against the previous year, although it is important to note that request volumes have increased by 33% when compared against the previous year.

Internal Reviews

36. Customers who submit a FOI EIR or Data Subject Access requests can request an internal review if they are not satisfied with the response provided. Internal reviews provide the Council with an opportunity to review the request handling process prior to any potential referral to the Information Commissioner's Office by the requester.

37. During 2022-23, the Council has processed the following Internal Reviews:

Internal Review Type:	2020/21	2021/22	Apr – Nov 2022
Freedom of Information	30	32	17
Environmental Information Regulations	3	0	0
Data Protection Act	14	10	5
Total	**47**	**42**	**22**

Referrals to the Information Commissioner's Office (ICO)

38. If an applicant is not satisfied with the outcome of an Internal Review, they can refer their case to the Information Commissioner, who will assess the case and make an independent decision about the way the council has handled the request.

39. The role of the Information Commissioner is to uphold information rights in the public interest. The ICO is the regulator for Freedom of Information, Environmental Information Regulations and the Data Protection Act. Part of the Information Commissioner role is to respond to complaints about the way local authorities have handled requests for information, make recommendations on best practice and take appropriate enforcement action. During 2022/23 the Council were notified of the following referrals to the Information Commissioner:

Referral Type to ICO	2020-21	2021-22	Apr – Dec 2022
Freedom of Information	3	5	7
Environmental Information	1	0	0
Data Protection Act	7	3	1
Total	**11**	**8**	**8**

40. Following a referral and a subsequent case investigation, the ICO can issue a Decision Notice requiring the Council to disclose information it may previously have refused to disclose. Details of all decisions received are monitored by the Data Protection Officer and reviewed by the SIRO Performance Group in tracking response progress as well as lessons learned where the Council may be found at fault with the actions it has taken.

41. A summary of the outcomes for 2022/23 is shown in the table below.

ICO Outcome:	No. cases.
No Further Action	7
Improvement Actions/Advice	0
Decision Notice	1
First Tier Tribunal	0

Referrals to the First Tier Tribunal (FTT)

42. If an applicant is dissatisfied with the Information Commissioner's decision, they have the right to refer the matter to the First Tier Tribunal (FTT). The council can also appeal fines issued for data breaches and enforcement notices to the FTT. The FTT is independent of the Information Commissioner and listens to representation from both parties before it reaches a decision. Any party wishing to appeal against an ICO Decision Notice has 28 days to do so.

43. During April – December 2022 the Council did not receive any referrals to the First Tier Tribunal:

Referral type to First Tier Tribunal	No cases April – Dec 2022	Outcome
Freedom of Information	0	Not applicable
Environmental Information	0	Not applicable
Data Protection Act	0	Not applicable

Charges

44. The Council has a charging policy and schedule of charges relating to FOI requests. The only fees that can be applied under FOI are for photocopying and postage, commonly referred to as disbursements. If the Council wishes to charge a fee for supplying information a Fees Notice must be issued to the applicant within the statutory timescale. Until the fee is paid, the Council is under no obligation to continue processing the request. For the year 2022/23, the Council did not issue any fee notices as all disclosures were provided by e-mail with relevant information attached if required.

Transparency and Open Data

45. The County Council is committed to complying with the Local Government Transparency Code 2015. The Council routinely publishes all data mandated by the Code with support from identified service specialists and is committed to proactively publish information relevant for the public.

46. Data is available in reusable format via the council's Open Data webpage via the following link:

http://www.cumbria.gov.uk/council-democracy/accesstoinformation/opendata/default.asp

Cumbria County Council transition to the new Cumberland and Westmorland & Furness Unitary Councils

47. As part of the County Council SIRO responsibilities, the SIRO, Deputy SIRO Officers, Data Protection Officer and wider ICT and Information Security professionals have invested significant time to ensure the County Council systems processes and security arrangements are in place to either transfer data from the County Council that is required for the business operations of Cumberland and Westmorland & Furness Unitary Councils.

48. Political leadership of information governance is vital to the success of the organisation and each of the two new Councils has a portfolio holder appointed at Cabinet / Executive level to champion the important role of Information, ICT and Security Management.

49. Both new Unitary Councils also have now made Director Level appointments which include the responsibility for SIRO as well as Chief Legal Officer (Monitoring Officer) appointments to support and ensure robust governance is in place to maintain the high standards set from sovereign organisations with any risks identified, managed and effectively controlled.

Conclusion

50. Despite the continuing challenges relating to information security, data protection and the increasing global challenges and threats relating to cyber attacks, progress has continued to be made during 2022/23 to ensure the Councils governance, procedures, culture, profile and defences are being maintained and improved, staff training and awareness is developed and delivered whilst at the same time ensuring the delivery of the services continues with strong information governance in place.

51. As this is the final SIRO report for Cumbria County Council before the Council ends on 31 March 2023, I would like to place on record my sincere thanks and appreciation for all the work, commitment and council wide cultural improvements the County Council has made as a result of elected members, officers and partners working together to protect data, information and ICT security and strive for best practice for the benefit and protection of the community we collectively serve.

Paul Robinson
Assistant Director Organisational Change
Interim Corporate Director Corporate Customer & Community Services
Cumbria County Council Senior Risk Information Owner (SIRO**)**

Further Information

For further information and guidance please contact:

Steve Tweedie
Information Governance & Investigations Coordinator
Email: steve.tweedie@cumbria.gov.uk

Translation services

If you require this document in another format (e.g. CD, audio cassette, Braille or large type) or in another language, please telephone 01228 606060.

আপনি যদি এই তথ্য আপনার নিজের ভাষায় পেতে চান তাহলে অনুগ্রহ করে **01228 606060** নম্বরে টেলিফোন করুন।

如果您希望通过母语了解此信息，
请致电 **01228 606060**

Jeigu norėtumėte gauti šią informaciją savo kalba, skambinkite telefonu 01228 606060

W celu uzyskania informacji w Państwa języku proszę zatelefonować pod numer 01228 606060

Se quiser aceder a esta informação na sua língua, telefone para o 01228 606060

Bu bilgiyi kendi dilinizde görmek istiyorsanız lütfen 01228 606060 numaralı telefonu arayınız