Cumbria County Council

2019/20 Annual Report

Senior Information Risk Owner (SIRO)

Information Governance - assurance and performance.

June 2020

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. It provides assurances that information risks are being effectively managed; what is going well; and where improvements are required.

The 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; 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 continues to present an increasing 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 and further activity planned to maintain and strengthen defenses and enhance corporate resilience.

Performance in relation to information requests processed under Freedom of Information (FOI) and Data Protection legislation is summarised in the report. The report also updates on the changes implemented to these services further to their transfer to the Service Centre and further actions planned to improve response performance.

The number of data breaches reported are also showing an increase compared with the number of incidents reported in the previous year. This area remains subject to continuous monitoring to identify learning or process changes that may be required to reduce the risk of further breaches occurring.

The report also updates on continuing actions taken in relation to the General Data Protection Regulations (GDPR) which came into force on the 25th May 2018.

Introduction

1. The Senior Information Risk Owner (SIRO) Annual Report reflects on the Council's information governance work undertaken during 2019-20, and 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. The Annual Report also provides an update on the action plans the Council has in place to minimise risk or improve performance.

3. Specifically, this report:

    a) 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:-

- Data Protection Act (1998) – replaced with General Data Protection Regulations (GDPR 2018)
- Freedom of Information Act (2000);
- Environmental Information Regulations (2004);
- Information Security Standard ISO/IEC 27002:2007;
- NHS IG - Data Security & Protection Toolkit (DS&P Toolkit).

b) Details any Serious Incidents Requiring Investigation (SIRI) within the preceding twelve months, relating to any losses of personal data or breaches of confidentiality.

Key Roles and Responsibilities

4. The Executive Director - Corporate, Customer and Community Services is the Council's Senior Information Risk Officer and is responsible for:

- Leadership and overall ownership of the Council's Corporate Governance Action Plan, acting as corporate champion for information governance;
- Providing a focus for the management of information governance at a senior level;
- Providing advice and reports in respect of information incidents and risks, including the content of the council's Annual Governance Statement relating to information 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;

5. There are a number of officers and teams across the Council that have professional expertise relating to information governance and information security, however it is 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.

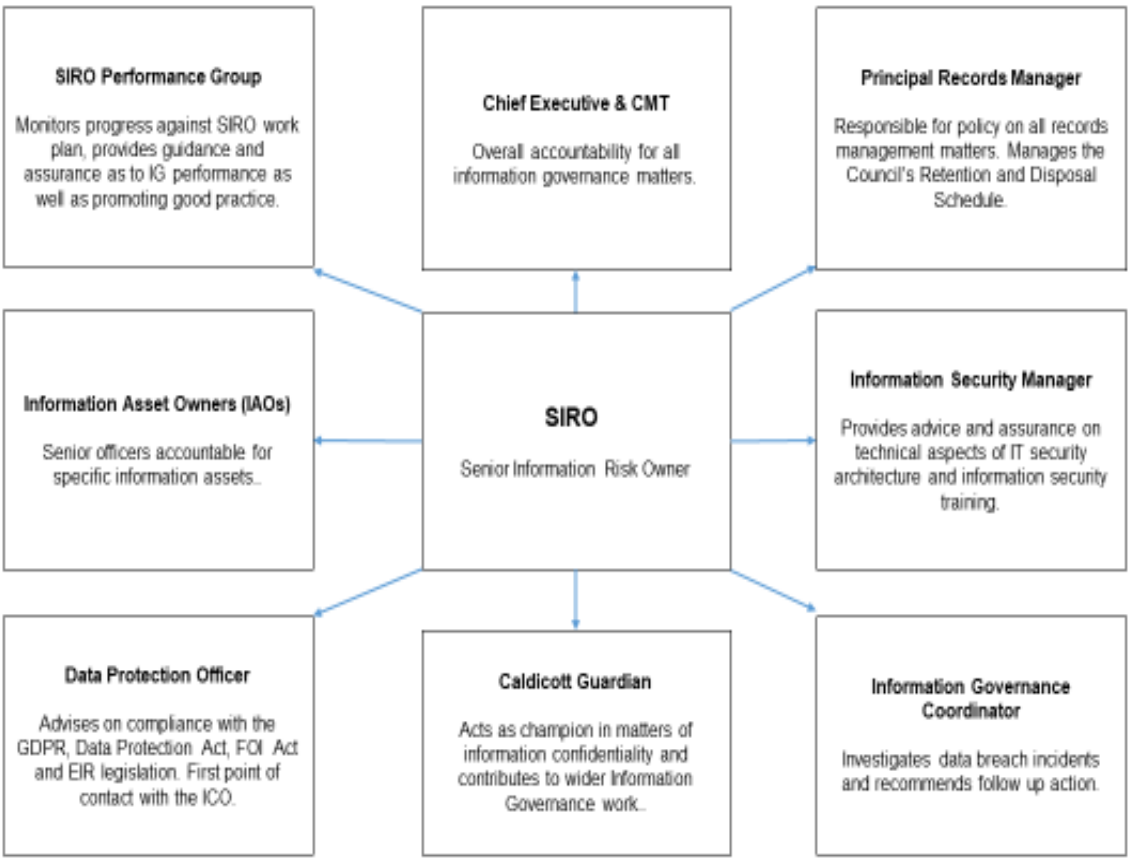
Governance and Monitoring Arrangements

6. The Council's SIRO is supported via the Corporate Governance Group (CGG) which is a strategic group that maintains oversight of information governance for the Council. In addition the 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 has been too:

- 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 to deliver the improvement plan;
- 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 PSN accreditation, 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 Data Controllers;
- Provide assurance that where there are changes in processes or working practices that appropriate information governance risk assessments or Privacy Impact Assessments (PIAs) are undertaken.

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



Risk Management and Assurance

7. The Council's Corporate Risk Register for 2019-20 has continued to include an Information Security Arrangements risk, which is a combination of Data Protection and ICT Cyber Security threats, and is described in the following manner:

   There is a risk that the Council will experience a significant information security incident. Due to Inadequate information security arrangements, lack of training, awareness & ongoing learning as well as Human error. Resulting in the 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, fines of up to 20 million euros or 4% of Gross budget, partial or total interruption to service delivery to customers, suppliers or partners impacting the partial or non-delivery of corporate priorities, significant reputational impact to the Council & partners, reputational damage to the Council and ultimately significant Financial consequences.

8. As part of the Council's governance and assurance arrangements, a quarterly corporate risk report is presented to Corporate Management Team, Cabinet Briefing and finally to the Audit & Assurance Committee meeting to provide a progress update on all of the corporate risks, including the Information Security Arrangements risk.

9. Throughout 2019/20 the risk rating for the Information Security Arrangements corporate risk has remained consistently high and had a risk score of 15 (impact of 5 and likelihood 3). This risk, alongside the other corporate risks, is reviewed on a quarterly basis to track any changes to the risk score and to monitor progress on the implementation of new or improved internal controls that support the ongoing management and mitigation of the risk.

   This risk also had a target end of year score of 10 (impact of 5 and likelihood 2), however due to a number of ongoing factors outlined below, the end of year risk score remained at 15.

   Ongoing ICT Cyber Security Threats
   - Cyber-attack internationally, nationally and regionally remains a high risk overall and the actual consequences of a cyber-security attack on the Council, if realised, would be significant and have a considerable impact across all Council Services.
   - 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 and these security controls have been independently assessed with positive progress acknowledged.

   Ongoing Data Protection Threat
   - Ongoing awareness raising and the mandatory completion of Information Security Training has progressively increased the number of reported data breaches and near misses.
   - On investigation of the data breaches, the majority are the result of human error rather than a systemic or governance failure and although further controls are being implemented to prevent recurrence, we have not yet achieved a sustained reduction in the number of data protection related breaches and near miss incidents.

Ongoing Impact of COVID-19

- During the fourth quarter of 2019/20, and particularly from early March 2020, the novel coronavirus (COVID-19) spread across Cumbria and had an immediate impact on the delivery of Council Services in general and ICT services in particular.
- A report was presented to CMT on 22 April 2020, with regard to the Corporate ICT and Information Security Position Statement in context of COVID-19, with the report highlighting a number of immediate Information Security concerns and business continuity response tactics;
    - There was an immediate increase in cyber-attacks and cyber fraud globally, nationally and regionally.
    - The revised flexible working environment and the need to social distance led to an increased reliance on the use of technology to maintain operations across the whole Council
    - Cumbria County Council remains fully committed to ICT and cyber security and has implemented significant additional resources and overcome a number of operational challenges to ensure the Council responds effectively to COVID-19. As an example, the number of employees working remotely using the corporate ICT solution is now around 5500 VPN connections per day with significant expansion in the number of ICT end user devices being deployed.

10. During 2020/21 and especially in context of COVID-19, an Information Security risk will remain on the corporate risk register to ensure we address the risks relating to accidental data loss, physical system failures and direct malicious cyber-attacks. There is an ongoing need for the Council to address all aspects of this risk through robust ICT and risk management processes as well as addressing the cultural and behavioural elements of this risk. As such this risk will be refreshed during Quarter 1 2020/21.

11. **Covid-19 actions in relation to Data Protection** has seen work undertaken by a range of colleagues/teams across the council and external/partner agencies, the list below provides an insight into this activity:

- Interpretation/Practical Application of:
    - Control of Patient Information (COPI) Notices issued by Department of Health and Social Care
    - Information Commissioner's Office (ICO): COVID19 Guidance
- Data Sharing Agreement/Privacy Notice/Data Collection Forms for the Multi-Agency Intelligence Cell (MAIC)
- Data Sharing Agreement/Privacy Notice for Cumbria COVID-19 Local Contact Tracing System
- Terms of Reference, Video Conferencing Guidance, Data Protection/Confidentiality Statements for the Business & Economic Response & Recovery Group (BERRG)/Cumbria Local Enterprise Partnership (CLEP)/Chamber of Commerce
- Data Sharing/Privacy and System Requirements for Emergency Support Helpline, Employee Coaching and Wellbeing Service and Employee Screening

12. The council's data protection response during COVID-19 has been influenced by the foundations laid by the Data Protection Working Group during the GDPR Implementation Project. Key procedures and processes have worked well and proved effective in recording and evidencing data protection issues and risks.

13. Also of note are the lessons learned by colleagues involved in the council's response to previous emergency situations, specifically in relation to data sharing obligations and documentation. Key procedures have proved adequate and supported the council's to comply with its data sharing requirements throughout the COVID-19 response.

Corporate Governance actions

14. The Council is committed to a clear strategy and sustainable framework for Information Governance across the Council. Quarterly performance reports were provided to the Corporate Management Team to enable continuous monitoring of the actions required to manage information issues, risks and cultural behaviour to improve the Council's arrangements around data handling, processing and security.

15. In summary, the following key actions were delivered in 2019-20 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 performance high of 92.9% was achieved of CCC staff available to undertake the training having completed the course. This is against the Council's target of 95%. A revised course for 2020 has been launched in July 2020 which includes lessons learned from data breaches that have been recorded. Completion of the course remains mandatory for all staff.

- The NHS requirement for an annual submission to be provided by the authority to show compliance with their Data Security & Protection Toolkit was suspended by the NHS in March due to the focus being on the Covid-19 response. The revised submission date is now 30th September 2020 with the Authority having provided its submission on the 10th July 2020.

- Successful compliance with the requirements for ongoing access to the national Public Service Network. (PSN) was achieved on July 12th 2019. This included approval by PSN of the Remediation Action Plan (RAP) to address the vulnerabilities highlighted within the annual IT Health Check (ITHC). Weekly updates were provided to PSN regarding progress of the actions highlighted.

- The Council's Senior Information Risk Owner chairs a weekly meeting to consider any data breach incidents deemed to be high risk and will advise on whether a self-referral of the incident to the Information Commissioner's Office (ICO) is appropriate.

- The Data Protection Working Group (DPWG) which oversees the work required in relation to this area has undertaken a review of the original Action Plan with ongoing actions now incorporated into a Data Protection Compliance Roadmap (DPCR).

  The DCPR is designed to achieve a number of outcomes as noted below and is supported by a series of workstreams with representatives from across a range of service areas:

  - Monitoring/implementation of legislative or regulatory changes (including Brexit implications);
  - Development/maintenance of compliant policies, procedures and systems;
  - Monitor, design and deliver an effective communication and training plan;
  - Providing assurance on GDPR/DPA compliance via a quarterly report in relation to progress of the DPCR.

- **Information Asset Register: (IAR):** A review has been completed of the existing IAR. An action plan for delivery of a revised register is now in place with early stage work commenced on its delivery. Initial stages will see an appropriate ICT solution identified which incorporates process automation.

Data Breach Management and Reporting

16. 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, the incident may need escalation to the Council SIRO and Caldicott Guardian, and 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.

17. All breaches and near misses are reported to the Senior Information Risk Owner (SIRO) on a weekly basis. Consideration is given to whether the incident should be referred to the Information Commissioner's Office (ICO). A total of eight cases were referred to the ICO in 2019-20. All these cases have since been closed by the ICO without any fines being applied. The ICO may make recommendations as a result of any investigations they undertake as to what actions they expect to be taken by the Authority.

18. During the period 2019-20, the Council recorded and investigated 224 potential data breaches. (In 2018-19 there were 174 investigations undertaken). The increase in recorded incidents can in the main be attributed to the wider awareness of data protection arrangements following the introduction of GDPR in May 2018. This not only applies to staff who have undertaken training on Information Security and the requirement to report incidents in a timely manner but also the awareness and understanding of service users as to the requirements to ensure their data is held securely. The category and numbers of each potential breach are outlined below. As noted above eight cases were self-referred to the ICO.

Category of Potential Breach	**Number 2018/19**	**2019/20**
Data posted or emailed to incorrect recipient	98	115
Failure to redact data	11	15
Loss / Theft of mobile device	3	8
Loss / Theft of paperwork	10	7
Data left in insecure location	6	11
Verbal disclosure	8	8
Near miss / Non event	8	0
Unauthorised system access	1	0
Failure to use 'Bcc' option when sending an email	1	3
Information uploaded to webpage	4	4
Unlawful disclosure of sensitive / personal data	11	10
Other failure	12	33
Insecure disposal of paperwork	0	1
Not applicable	1	9
Total	**174**	**224**

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

Risk Rating	**Number recorded**
0- No Loss	41
1- Low Risk	83
2- Medium Risk	89
3- High Risk	11
Total Breaches	**224**

20. Learning from breaches: As part of the investigation of an incident, learning actions will be 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.

21. Learning is shared across the organisation via team briefings advising of incidents as well as corporate messages being issued to staff to remind them of good practice in avoiding breaches occurring.

ICT Security & Cyber Risks

22. The use of digital information and networks continues to grow and provides the foundation on which front line services are delivered. Cyber security continues to be a Tier 1 risk to national security. “Hostile attacks upon UK cyber space by other states and large scale cybercrime”. As such it remains of high importance and corporate priority.

23. The type of risks include theft of sensitive corporate or personal data, theft or damage to data, threat of hacking for criminal or fraud purposes and potential denial of service disruption to council ICT systems, intranet, mobile smart devices, public facing websites and misinformation.

24. Cumbria County Council continues to adopt the “10 Steps to Cyber Security” from the National Cyber Security Centre (NCSC), which is actively promoted and maintained. This guidance, when implemented reduces the risk to organisations. To reduce the risk still further the Authority has adopted the following approaches:

25. The Council subscribes to and proactively participates in the iNetwork – North West Warning, Advice and Reporting Point (NW WARP). The Information Security Manager is now a member of the Leadership Team of the NW WARP. This group continually reviews cyber threat situational awareness and acts as a reporting and escalation mechanism for cyber incidents as well as providing mutual help, guidance and peer review. It is supported by the NCSC and facilitates access to the Head of PSN and to national cyber security expertise and support.

26. The Council presence on the external, public internet is registered and monitored by the NCSC, GCHQ, Cyber Security Information Sharing Partnership (CiSP). Alerts are provided to Cumbria County Council when suspicious activity is identified or has been blocked.

27. As part of the commitment to the “10 Steps to Cyber Security” a robust patching regime is in place. All software updates are promptly installed after robust testing to ensure no negative impact upon the security of information or to the ICT service.

28. Internal vulnerability scanning continues on a 24/7 basis using industry standard scanning tools. All vulnerabilities identified are logged, prioritised and progressed within ICT. All critical vulnerabilities discovered are raised immediately with the ICT Management team. Once remediated each vulnerability is then re-scanned to provide assurance that the remediation has been successful.

29. Information security and cyber security technical controls are embedded into the procurement of new or replacement ICT systems.

30. All ICT contracts contain provision for information security and they include the Council’s expectations within the context of reducing the cyber risk both internally and externally hosted systems.

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

31. During 2019-20 the Council received 1487 requests for information under the Freedom of Information Act and the Environmental Information Regulations. This represents a 5% decrease in requests compared with 2018-19 figure of 1573.

Year	Requests Received	Processed on time	Performance (Target (90%)
2017/18	1337	1098	82%
2018/19	1573	1122	71%
2019/20	1487	1070	72%

32. The Council responded to 72% (1070) requests within the statutory time limit of 20 working days which represents a slight increase in performance compared with 2018-19 (71%). It should be noted that due to the impact of Covid-19 both on organisation working, services and Cumbria residents and communities it was agreed not to pursue front line services for FOI responses during this period.

33. The Complaints and Information Governance Team had a change of management in August 2019. This was part of a wider project lead by Alison Graham, Service Centre Manager to transition the Information Governance Team to Service Centre Management and relocate to the Parkhouse Building.

34. A project group was established to support the transition and to implement new ways of working and service improvements through service redesign. A full review of the IG and Complaints processes was undertaken with the Digital Team and key stakeholders to provide new technology to improve performance.

35. In March 2020 the IG Team began using the MATS system for logging and managing FOI / EIR requests. MATS provides the team with much improved functionality. Time spent logging new requests has been drastically reduced and the system sends automated emails both internally and externally. MATS also sends automated reminder prompts to Officers which helps the team manage deadlines and monitor progress. .

36. Work has commenced to explore consistent and appropriate reporting / tracking of requests. The MATS system provides the opportunity to run data enquiries, real-time statistics and automated reporting. Reports showing new / open cases are sent to Directorates weekly to ensure they are kept up-to-date with outstanding enquiries.

Data Protection Act (DPA) – Replaced with GDPR May 2018.

37. 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 Subject Access Request (SAR). In the last three years the council has handled the following requests. The performance shown for 2017-18 is against the target to process 75% within 40 days. Following the introduction of GDPR in May 2018 the target to process is now 75% within one calendar month which is reflected in the 2018-19 & 2019-20 figures shown.

	2017/18	**2018/19**	**2019/20**
Requests Received	157	190	330
Actioned within 1 Month (Number)*	101	139	184
Within 1 Month (%)*	64%	73%	56%

*The performance figures for 2017-18 are based on responses provided within 40 calendar days.

38. The Information Governance Team based within the Service Centre receives and handles requests for data in relation to Children and People Management. People Management previously handled requests for personnel data of current staff or former employees but this is now undertaken by the IG team. Adult Social Care records are allocated to the appropriate service area for processing.

39. During 2019-20 the demand for Subject Access requests has continued to increase substantially. There has been a 79% increase in requests over the year. This substantial increase in demand has proved challenging in terms of maintaining the performance target. A decision as to the processing and handling of requests, based on the service review undertaken on this service area earlier this year is to be undertaken, as noted I the action plan for 2020/21 below.

Internal Reviews

40. Customers who submit a FOI EIR or Subject Access request 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. During 2019-20, the Council has processed the following Internal Reviews:

Internal Review Type:	**2017/18**	**2018/19**	**2019/20**
Freedom of Information	32	28	24
Environmental Information Regulations	1	4	5
Data Protection Act	5	2	17

Referrals to the Information Commissioner's Office (ICO)

41. 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.

42. 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 2019-20 the Council were notified of the following referrals to the Information Commissioner:

Referral Type to ICO	2017-18	2018-19	2019-20
Freedom of Information	8	5	3
Environmental Information	1	2	0
Data Protection Act	9	3	10

43. 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.

Referrals to the First Tier Tribunal (FTT)

44. 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.

45. During 2019-20 the Council did not receive or make any referrals to the First Tier Tribunal:

Referral type to FTT	2019-20	Outcome
Freedom of Information	0	Not applicable
Environmental Information	0	Not applicable
Data Protection Act	0	Not applicable

Charges

46. 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 2019-20 the Council did not issue any fee notices as all disclosures were provided by e-mail with relevant information attached if required.

Exemptions

47. Both the Freedom of Information Act and Environmental Information Regulations contain exemptions that allow the council to withhold specific information for example if it is commercially or legally privileged. When the Council wishes to rely on an exemption, the applicant must be issued with a Refusal Notice within the relevant statutory timescale.

48. The Council cannot charge for the provision of information, however if it is estimated that a request will incur unreasonable cost then it can issue a Refusal Notice under Section 12 of the Act. The threshold set by the Act is 18 hours (equivalent to £450 at a notional hourly rate of £25).

49. To reach a decision about whether or not to apply a Section 12 exemption, the Information Governance Team works with the service area to estimate the expected time to:
- determine whether the information is held;
- locate information or appropriate documents;
- retrieve the information or document containing it;
- extract the information;
- process the request.

50. During 2019-20 the Council applied an exemption to 124 requests and the breakdown for type of exemption and times applied is presented below.

Exemption	**Times Applied**
Section 09 – Fee Notice	1
Section 12 - Exceeds Cost Limit	50
Section 14 - Vexatious or Repeated	1
Section 21 – Reasonably Accessible by other means	38
Section 22 - Future Publication	6
Section 23/24 – Security Bodies / National Security	0
Section 30 - Investigations conducted by Public Authority	0
Section 31 – Law Enforcement	0
Section 39 – Environmental Information	0
Section 40 – Personal Data	19
Section 41 – Confidentiality	0
Section 42 – Legally Privileged	0
Section 43 – Commercially Sensitive	9
Section 44 – Prohibitions on Disclosure	0
Total	**124**

Service Costs

51. The estimated cost of providing the Information Governance service relating to FOI and EIR handling is made up of two process elements:

- time taken by officers in Directorates to process requests for information under FOI and EIR; and locate and retrieve information.

- the cost of a centralised team that manages and advises (e.g. on the application of exemptions and exceptions), support to prepare disclosures, quality assurance advice on the content of disclosures, and maintenance of the Council's Publication Scheme.

52. The table below sets out a comparison of costs over the last 3 years. It should be noted the central team has wider responsibilities, including complaints and training; and undertakes a much wider range of activity than processing requests.

	2017-18	**2018-19**	**2019-20**
Total Number of Requests	1337	1593	1487
Estimated cost of processing in Directorates	£199,175	£214,475	£212,925
Cost of the Central Team	£102,111	£109,910	£87,624
Total estimated cost	£301,286	£323,664	£300,549
FTE in Central Team	2.5	3.2	2.0
Estimated unit cost per request	£226	£203	£202
ICO threshold for refusal per request	£450	£450	£450

Transparency and Open Data

53. The 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.

54. 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

Action Plan for 2020/21

55. The following actions have been identified for 2020/21 to further strengthen the Council's information governance arrangements.

Plan Ref:	Priority area	Current position	Action	Officer Responsible	Completion target date
001	**FOI/EIR PERFORMANCE**	A case management model of working has been begun to be implemented which supports effective monitoring, a targeted service approach with support and clearer accountability for progress.	Apply the case management approach and system consistently across all Directorates.	Alison Graham	31/12/2020
002	**FOI/EIR PERFORMANCE**:	The team have excellent working relationships with all Directorates, and recognise that the service turnaround time is the key factor in improving performance.	Develop and deliver workshops, an online survey and small group remote training sessions to improve service turnaround and timeliness.	Alison Graham	31/12/2020
003	**FOI/EIR PERFORMANCE**:	Reporting tools are being reviewed to ensure that the right information is going to the right people and is being used to drive improvement. The MATS system provides the opportunity to run data enquiries and real-time automated reporting. Reports showing new / open cases are sent to Directorates which will be incorporated into the training and workshops to ensure they are utilised efficiently to support further improvements in timely responses to FOIs and EIRs.	Undertake a full review of reporting arrangements to identify and implement improvements to support greater management oversight and overall performance improvement.	Alison Graham	31/12/2020

Plan Ref:	Priority area	Current position	Action	Officer Responsible	Completion target date
004	**Subject Access Request (SAR) performance.**	A review of the SAR handling process has been undertaken as part of the phased approach to redesigning the service following its transfer to the Service Centre. The volume of requests has increased significantly over the last 12 months which requires additional capacity to be identified and full training.	Progress the recommendations of the review through Corporate Customer and Communities DMT.	Alison Graham	30/09/2020
005	**Creation of a Cumbria Cyber Resilience Group.**	Partners include organisations from both the public and private sectors including BAE Systems, Sellafield, private utility companies and Cumbria Constabulary who combined create a significant cyber resource pool of expertise and knowledge. Creating this Group will enable a multi-agency response to cyber incidents within Cumbria.	Develop a new Cumbria Cyber Resilience Group, by working with the lead body (Cumbria Police) and through the Local Resilience Forum (LRF).	Ian Smith	31/03/2021
006	**Privacy Notices.**	Privacy Notices explain what data the council will collect, who it will be shared with, why we need it and how it will be used. The council is committed to continually reviewing and updating its privacy notice to reflect service changes, feedback from customers and changes in the law.	Undertake a review of Privacy Notices to ensure they reflect current requirements.	Claire Owen	30/09/2020

Plan Ref:	Priority area	Current position	Action	Officer Responsible	Completion target date
007	**CCTV and Surveillance.**	Further to responding to a survey from the Surveillance Camera Commissioner (SCC) the Council's Data Protection Officer has been confirmed as the Senior Responsible Officer (SRO) for the work required to ensure the Council's compliance with its responsibilities in this area of work.	Develop a CCTV and Surveillance Action Plan in response to the survey submission.	Claire Owen	31/10/2020
008	**Data Sharing Agreements**	Work in relation to Data Sharing agreements has been maintained during 2019-20 but is to be subject to a full process review.	Carry out a full review of Data Sharing Agreements, focusing on the process in place for the creation of agreements, monitoring arrangements, and to include learning from Covid-19.	Claire Owen	31/12/2020

Steve Tweedie, Information Governance & Investigations Coordinator

25 August 2020

Conclusion

56. In summary, progress has been made during 2019-20 with key actions taken to strengthen the Council's approach to effectively manage information risks and ensure a robust approach to information governance.

57. In particular, as the potential for cyber risk increases, it is essential the Council takes action to understand and mitigate risk in this area.

Dawn Roberts
Executive Director – Corporate, Customer and Community Services

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