Cumbria County Council

2020/21 Annual Report

Senior Information Risk Owner (SIRO)

Information Governance - assurance and performance.

August 2021

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.

Whilst the year has seen many changes in working practices and additions of new technology as a result of COVID-19, 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, 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 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 to maintain and strengthen defenses and enhance corporate resilience.

Achievements in the past year include:

- The implementation of a new system to handle Freedom of Information requests (FOIs) resulting in an increased level of performance for response being provided within 20 working days to 83%. (Previous year 72%). N.B. For the 3 month period January-March 2021 performance achieved was 91%
- A review of the approach to handling subject access requests (SARs) increasing performance to 67% of cases handled within one calendar month. (Previous year 56%).
- A decrease in the number of data breach cases self-referred to the Information Commissioner's Office (ICO) to two. (Previous year 8).
- 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.
- A Cumbria Cyber Resilience Group has been developed through working with the lead body (Cumbria Police) and through the Local Resilience Forum (LRF).
- A review of all existing documentation used for the planning, monitoring, and reporting of compliance with data protection legislation has been undertaken.
- A review of the Council's Corporate Privacy Notice has been undertaken, all external content has been updated and internal guidance published for employees.
- Information Asset Register (IAR) work is continuing on the development and improvement of the Council's Information Asset Register. The register was made available to all asset owners on the 15th January 2021 via SharePoint Online

The report also updates on the Council's actions on building a robust data protection compliance programme further to the General Data Protection Regulations (GDPR) becoming incorporated into domestic law as the UKGDPR on the 1st January 2021.

Introduction

1. The Senior Information Risk Owner (SIRO) Annual Report reflects on the Council's information governance work undertaken during 2020-21, 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 actions the Council had in place for 2020-21 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:-

- UK General Data Protection Regulation (UK GDPR);
- 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 data breaches 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;

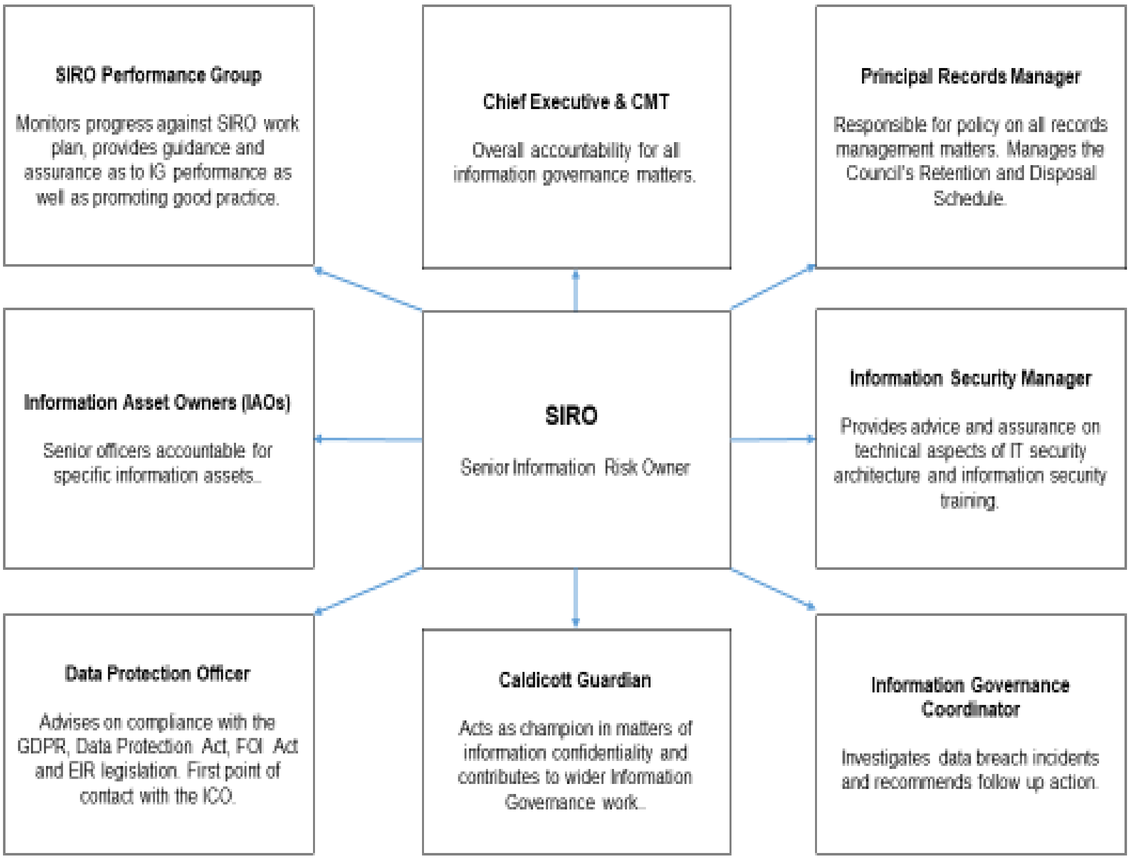
5. There are a number of officers and teams across the Council that have professional expertise relating to information governance and information security, however it is important that information governance must be everyone's business, with all staff and elected members having personal responsibility 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 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 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;
- 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 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.


SIRO Performance Group
Monitors progress against SIRO work plan, provides guidance and assurance as to IG performance as well as promoting good practice.
Chief Executive & CMT
Overall accountability for all information governance matters.
Principal Records Manager
Responsible for policy on all records management matters. Manages the Council's Retention and Disposal Schedule.
Information Asset Owners (IAOs)
Senior officers accountable for specific information assets.
SIRO
Senior Information Risk Owner
Information Security Manager
Provides advice and assurance on technical aspects of IT security architecture and information security training.
Data Protection Officer
Advises on compliance with the GDPR, Data Protection Act, FOI Act and EIR legislation. First point of contact with the ICO.
Caldicott Guardian
Acts as champion in matters of information confidentiality and contributes to wider Information Governance work.
Information Governance Coordinator
Investigates data breach incidents and recommends follow up action.

Risk Management and Assurance

7. The Council's Corporate Risk Register for 2020-21 has continued to include an Information Security Arrangements risk, which is a combination of Data Protection and ICT Cyber Security threats. This takes account of the separate requirements of the UK GDPR to implement effective technical and organisational measures to protect personal data. The risks is described as follows:

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

This may arise due to;

- inadequate arrangements in respect of information security, data protection and surveillance cameras.
- Lack of training, awareness and ongoing learning.
- Human error.

Resulting 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.

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 2020/21 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.

Ongoing ICT Cyber Security Threats

- Cyber-attack internationally, nationally (Hackney, Redcar & Cleveland) and regionally (Newcastle and Northumbria University) 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 seen a reduction in data breaches and near misses (as noted in the table below) being reported throughout the year.
- On investigation of the data breaches, the majority are the result of human error rather than a systemic or governance failure. Where appropriate any learning from breaches is implemented to reduce the risk of a similar recurrence.

Impact of COVID-19

- During 2020/21 (COVID-19) spread across Cumbria and had an immediate impact on the delivery of Council Services in general and ICT services in particular. This has seen the implementation of significant additional resources to overcome a number of operational challenges. Changes implemented have seen;
  - The number of employees working remotely using the corporate ICT solution increase to around 5500 VPN connections per day with significant expansion in the number of ICT end user devices being deployed.
  - A revised flexible working environment implemented to incorporate the need to social distance which has led to an increased reliance on the use of technology to maintain operations across the whole Council.

10. **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 Council's Data Protection Officer continues to monitor the implications and practical application of the Control of Patient Information (COPI) Notices issued by Department of Health and Social Care and advice issued via the ICO Data Protection and Coronavirus Information HUB.

11. The Council's response to the data processing challenges posed by COVID-19 remains ongoing and whilst operating effectively to identify and manage operational issues, areas of further growth and innovation are also being continuously monitored.

Corporate Governance actions

12. The Council is committed to a clear strategy and sustainable framework for Information Governance across the Council. 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.

13. In summary, the following key actions were delivered in 2020-21 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 83.2% 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 2021 has been launched in March, 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.

- The NHS requirement for an annual submission to be provided by the authority to show compliance with their Data Security & Protection Toolkit was submitted on the 10th July 2020.

- Successful compliance with the requirements for ongoing access to the national Public Service Network. (PSN) was acknowledged by PSN on the 19th March 2021 with receipt of the PSN connection compliance certificate for a further 12 months. This is a significant achievement given the additional challenges placed upon ICT whilst supporting the Council's COVID-19 pandemic response.

- A review of process and reporting arrangements with regard to Freedom of Information Act (FOIA) requests was undertaken. Further to the review the implementation of the changes, which included the implementation of a case manager approach, has seen an improvement in the time taken to provide responses to requests. Performance in relation to the handling of requests is detailed in this report.

- A review of Data Subject Access Requests (DSARs) handling was also undertaken. This review identified the requirement for additional resource being required to support the process. The resource have since been identified, recruited and trained. DSAR performance handling is also detailed in this report.

- A Cumbria Cyber Resilience Group has been developed through working with the lead body (Cumbria Police) and through the Local Resilience Forum (LRF). The development means Cyber warnings and alerts are regularly posted and discussed within the secure Resilience Direct multi agency platform. In the event of a Cyber-attack Cumbria County Council will be able to draw upon knowledge, expertise and experience from within the group and also provide mutual support when required. Cyber incident exercises are currently being planned, which will include members of the Cumbria Cyber Resilience Group within the Cumbria Local Resilience Forum (LRF).

- During 2020-21, a review of all existing documentation used for the planning, monitoring, and reporting of compliance with data protection legislation has been undertaken. The review highlighted several issues with a proposal that all data protection activity is recorded via the Data Protection Accountability Framework – Self-Assessment and Activity Tracker. This approach not only provides greater clarity and assurance to the SIRO, it assists with governance and reporting requirements, and most importantly complies with the minimum expectations of the Information Commissioner. A summary of findings from the Self-Assessment will be incorporated into the 2021-22 SIRO Annual Report.

- Privacy Notices: A review of the Council's Corporate Privacy Notice has been undertaken, all external content has been updated and internal guidance published for employees.

- Policies: The Data Breach Reporting Policy, Procedure and FAQs and GDPR Compliance Policy have been reviewed by the SIRO Group and republished.

- Information Asset Register: (IAR): Work is continuing on the development and improvement of the Council's Information Asset Register. The register was made available to all asset owners 15th January 2021 via SharePoint Online and all Information Asset Owners (IAOs) have confirmed their key information asset register entries. IAO training options have been researched and a plan is being established for their deployment and delivery.

- The Council's Internal Audit Service undertook an audit of 'Data Protection Compliance' which has resulted in a number of recommendations as to further actions to improve compliance. The 'Management Action Plan' setting out how any outstanding recommendations are to be implemented is currently being finalised.

Data Breach Management and Reporting

14. 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.

15. 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 two cases were referred to the ICO in 2020-21. (Down from eight in 2019-20). One case has since been closed by the ICO without any fines being applied. The outcome of the ICO's consideration of the second case is still awaited. 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.

16. During the period 2020-21, the Council recorded and investigated 204 potential data breaches. (In 2019-20 there were 224 investigations undertaken). The high number of incidents reported 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 two cases were self-referred to the ICO.

Category of Potential Breach	**Number 2019/20**	**2020/21**
Data posted or emailed to incorrect recipient	115	130
Failure to redact data	15	2
Loss / Theft of mobile device	8	1
Loss / Theft of paperwork	7	2
Data left in insecure location	11	6
Verbal disclosure	8	6
Near miss / Non event	0	0
Unauthorised system access	0	8
Failure to use ‘Bcc’ option when sending an email	3	1
Information uploaded to webpage	4	5
Unlawful disclosure of sensitive / personal data	10	29
Other failure	33	6
Insecure disposal of paperwork	1	0
Not applicable	9	8
Total	**224**	**204**

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

Risk Rating	**Number recorded 19/20**	**Number recorded 20/21**
0- No Loss	41	75
1- Low Risk	83	87
2- Medium Risk	89	41
3- High Risk	11	1
Total Breaches	**224**	**204**

18. Learning from breaches: 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.

19. 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.

ICT Security & Cyber Risks

20. 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.

21. 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.

22. 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:

23. 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.

24. 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.

25. 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. Over the past 12 months an increasing number of emergency cyber alerts have been received, which have required immediate software upgrades to be applied. These were facilitated using the existing emergency request for change process within ICT ensuring that all changes remain subject to the same technical review rigour as normal upgrades.

26. 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.

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

28. 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)

29. During 2020-21 the Council received 1209 requests for information under the Freedom of Information Act and the Environmental Information Regulations. This represents a marked reduction in requests compared with 2019-20 figure of 1487.

Year	Requests Received	Processed on time	Performance (Target (90%)
2018/19	1573	1122	71%
2019/20	1487	1070	72%
2020/21	1209	1002	83%

30. The Council responded to 83% (1002) requests within the statutory time limit of 20 working days which represents an 11% increase in performance compared with 2019-20 (72%). It should be noted that due to the impact of COVID-19 on operations, services and Cumbrian residents, it was agreed not to pursue front line services in the early period of the COVID-19 response work for FOI responses.

31. In March 2020 the IG Team began using the Liberty Create system for logging and managing FOI / EIR requests. Liberty Create (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. Liberty Create also sends automated reminder prompts to Officers which helps the team manage deadlines and monitor progress.

32. As noted at point 13 above a further review of the new technology has seen the implementation of a case-management approach and training for staff who handle the requests, resulting in improved response handling time. For the 3 month period January-March 2021 performance achieved was 91% with 295 of 325 requests being responded to within 20 working days,

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.

	2018/19	**2019/20**	**2020/21**
Requests Received	190	330	224
Actioned within 1 Month	139	184	151
Within 1 Month (%)	73%	56%	67%

34. The Information Governance (IG) 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. As noted in point 13 above during 2020-21 a review of the DSAR process was undertaken. This review identified the requirement for additional resource being required to support the process. The resource has since been identified, recruited and trained.

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. During 2020-21, the Council has processed the following Internal Reviews:

Internal Review Type:	2018/19	2019/20	2020/21
Freedom of Information	28	24	30
Environmental Information Regulations	4	5	3
Data Protection Act	2	17	14

Referrals to the Information Commissioner's Office (ICO)

37. 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.

38. 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 2020-21 the Council were notified of the following referrals to the Information Commissioner:

Referral Type to ICO	2018-19	2019-20	2020-21
Freedom of Information	5	3	3
Environmental Information	2	0	1
Data Protection Act	3	10	7

39. 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)

40. 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.

41. During 2020-21 the Council did not receive or make any referrals to the First Tier Tribunal:

Referral type to FTT	2020-21	Outcome
Freedom of Information	0	Not applicable
Environmental Information	0	Not applicable
Data Protection Act	0	Not applicable

Charges

42. 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 2020-21 the Council did not issue any fee notices as all disclosures were provided by e-mail with relevant information attached if required.

Exemptions

43. 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.

44. 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).

45. 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.

46. *During 2020-21 the Council applied an exemption to 67 requests and the breakdown for type of exemption and times applied is presented below.*

Exemption	***Times Applied***
Section 09 – Fee Notice	*0*
Section 12 - Exceeds Cost Limit	*18*
Section 14 - Vexatious or Repeated	*1*
Section 21 – Reasonably Accessible by other means	*35*
Section 22 - Future Publication	*5*
Section 23/24 – Security Bodies / National Security	*1*
Section 30 - Investigations conducted by Public Authority	*0*
Section 31 – Law Enforcement	*1*
Section 39 – Environmental Information	*0*
Section 40 – Personal Data	*3*
Section 41 – Confidentiality	*0*
Section 42 – Legally Privileged	*1*
Section 43 – Commercially Sensitive	*2*
Section 44 – Prohibitions on Disclosure	*0*
Total	***67***

Transparency and Open Data

47. 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.

48. 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

Conclusion

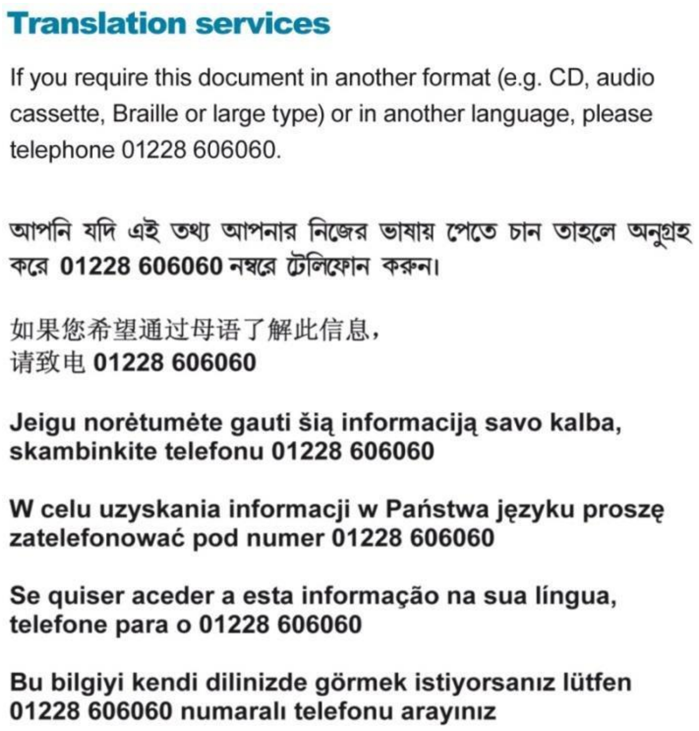
49. In summary, despite the additional challenges and disruption caused as a result of COVID-19, progress has been made during 2020-21 to ensure a continuing robust approach with regard to information governance arrangements. As well as existing actions and defences being maintained, additional actions as highlighted in the report, have been implemented to further strengthen the Council's approach.

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