Senior Information Risk Owner (SIRO)
Information Governance - assurance and performance.

June 2018
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 report outlines new and emerging information governance considerations, including actions taken in ensuring compliance with the new General Data Protection Regulations (GDPR) which came into force on the 25th May 2018 and the action plans the Council has in place to minimise risk and improve performance.

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 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 defences and enhance corporate resilience.

Performance in relation to information requests processed under Freedom of Information and Data Protection legislation is summarised in the report and whilst the Council has made performance improvements over the past year, this will continue to be an area of focus as additional improvement is required during 2018/19.
Introduction

1. The Senior Information Risk Owner (SIRO) Annual Report reflects on the Council’s information governance work undertaken during 2017-18, 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 a forward look at new and emerging information governance considerations for the Council, including preparations needed to ensure compliance with planned changes to legislation and the action plans the Council has in place to minimise risk or improve performance.

3. Specifically, this report:

   - 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:-
     - Freedom of Information Act (2000);
     - Environmental Information Regulations (2004);
     - Information Governance Toolkit.

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

   - Reports on the key achievements of the Corporate Governance Group Improvement Plan during 2017-18 and to outline actions planned for 2018-19.

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 Corporate Governance Group (CGG) is a strategic group that maintains oversight of information governance for the Council. Regular reports are made from the CGG to the Executive Director Corporate, Customer & Community Services as the SIRO. The CGG meets on a regular basis and members of the group adopt a strategic role in promoting and embedding good information governance. They are the champions for information governance in their respective directorates and develop a culture that values, protects and uses information to deliver improved services. More specifically the responsibilities of the CGG 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;
- Ensure there is a Corporate Governance Action Plan in place; to oversee its implementation; and to ensure its effectiveness;
- 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 Information Governance 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;
- Provide the main point of reference and escalation for the management of issues and risks related to information governance;
- 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 2017-18 contained a risk entitled ‘Inadequate Information Governance’ and is defined as:

“There is a risk that the Council breaches the Data Protection Act due to a loss of information, caused by ineffective data security, insecure data connectivity, insecure sharing arrangements with partners and external organisations, a cyber-attack and a lack of awareness and training, resulting in financial and reputational damage.”

8. Throughout 2017-18, the information governance risk continued to be assessed as high with the risk rated ‘likely’ and could have ‘severe impact’ on the Council as measured against the Council’s strategic risk management assessment criteria. The risk continues to be monitored on a quarterly basis with positive steps taken to mitigate the risk reported as part of the risk management and assurance reporting procedures which are presented to Corporate Management Team, Cabinet Members and the Audit and Assurance Committee.

9. Going forward, information governance and cyber risk are considered to be significant risk areas for all organisations locally, nationally and globally, with risks of accidental data loss, physical system failures and direct malicious cyber-attacks an ongoing area requiring focus. 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 remain on the Corporate Risk Register for 2018-19.

Corporate Governance Action Plan

10. The Corporate Governance Action Plan is in place to support ongoing improvement and the Council has continued to make progress throughout 2017-18.

11. The Council is committed to a clear strategy and sustainable framework for Information Governance across the Council and the Action Plan enables 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.

12. In summary, the following key actions were delivered which have strengthened the Council’s management of information risks:

- Completed delivery of Part 1 and Part 2 of the Corporate Governance training sessions for senior managers which saw 134 managers attending Part 1 with 112 attending Part 2. Part 1 focused on the purpose of corporate governance and what can go wrong if not followed. Part 2 focused on the democratic and decision making process, scheme of delegation, whistleblowing and fraud.

- 84.69% of ICT Users successfully completed their information security training against our target of 95%, with an overall completion rate of 69.96% when incorporating non ICT Users. A revised GDPR training programme has been developed and is a mandatory course for all staff and elected members for 2018;

- Implementation of automatic weekly reminders to staff not having completed training in the last 12 months.

- Annual submission for compliance to the Information Governance Toolkit at the end of March 2018;

- Successful compliance with the requirements for ongoing access to the national Public Service Network (PSN) on the 5th April 2018.

- New improved version of the Digital Mail Room installed at Cumbria House in January 2018.

- General Data Protection Regulation (GDPR) working group created to oversee the implementation of the new requirements.

- A dedicated ICT Security Engineer now in place to improve network security by proactively monitoring and tightening controls on a daily basis.
13. Progress has also been made with the following actions, with further work planned during 2018/19;

- Development of an Information Asset Register and the identification of information asset owners.
- Detailed refresh of the Council Records and Retention Schedules.
- Policy review and consolidation.
- Introduction of a revised information security training module incorporating requirements of the new GDPR.

**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 Guardians, and may be self-referred by the Council to the Information Commissioners Office (ICO). The reporting, attempt to recover, 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 Corporate Governance Group. Consideration is given to what happened, action taken to address the breach or near miss, a record of learning points and also action undertaken to avoid future occurrences.

16. During the period 2017-18, the Council recorded and investigated 65 potential data breaches. The category and numbers of each potential breach are outlined below. One case was self-referred to the Information Commissioners office.

<table>
<thead>
<tr>
<th>Number of cases</th>
<th>Category of Potential Breach</th>
</tr>
</thead>
<tbody>
<tr>
<td>15</td>
<td>Information disclosure - paper</td>
</tr>
<tr>
<td>12</td>
<td>Information disclosure - electronic</td>
</tr>
<tr>
<td>8</td>
<td>Failure to redact information</td>
</tr>
<tr>
<td>1</td>
<td>Loss / Theft of data</td>
</tr>
<tr>
<td>8</td>
<td>Other ‘principle 7’ failure</td>
</tr>
<tr>
<td>9</td>
<td>Verbal disclosure</td>
</tr>
<tr>
<td>12</td>
<td>Near miss / Non event</td>
</tr>
<tr>
<td><strong>Total: 65</strong></td>
<td></td>
</tr>
</tbody>
</table>

**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.

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.

The Corporate Governance Group have also requested a task and finish group be convened to review the recorded breaches in further detail to identify any trends where further action can be taken to mitigate the risk of similar breaches occurring in the future. The Council Monitoring Officer chairs this task and finish group.
ICT Security & Cyber Risks

17. As the importance of digital information and networks grows, cyber security is of high importance and remains a corporate priority. The type of risks posed include theft of sensitive corporate and personal data, theft or damage to data, threat of hacking for criminal or fraud purposes and potential disruption to infrastructure such as council ICT systems, intranet, and public facing website.

A presentation on Cyber Risk & Information Governance was made to the Audit & Assurance Committee on the 5th January 2018 by the Assistant Director - Business Services. Members challenged a number of areas and sought assurance as to arrangements in place to mitigate risks as to ‘personal failure’ to protect data and controls in place to protect systems and building security. An action was also identified to provide training in relation to social media platforms to ensure their use did not expose the Council to a cyber attack.

18. The National Cyber Security Centre (NCSC) has advised that Cyber risk has been increasing and for a number of years have been promoting the adoption of the “10 steps to Cyber Security”. This guidance, when implemented reduces the risk to organisations and has been implemented by Cumbria County Council.

To reduce the risk further, the Council has adopted the following approaches:

- Full compliance with the Public Sector Network (PSN) accreditation programme. Cumbria County Council were awarded PSN accreditation in September 2016 and have received re-accreditation in April 2018.
- The Council subscribes to and proactively participates in the iNETWORK – North West Warning, Advice and Reporting Point (NW WARP). This is a group that constantly reviews cyber situational awareness and acts as a reporting mechanism for cyber incidents as well as providing mutual help and guidance. It is supported by the NCSC which provides access to the Head of PSN and also facilitates access to national cyber security experts.
- The Council presence on the external, public internet is registered and monitored by the NCSC, GCHQ, Cyber Security Information Sharing Partnership (CiSP).
- A robust “patching” regime is in place. Software updates are promptly installed on all hardware after robust testing has been carried out to ensure there is no negative impact to the ICT service.
- Tracking mechanisms placed on all devices along with the use of specialist anti-cyber tools.

19. As the external cyber threat continues to increase, the ICT service must continually evolve to respond to a fast changing environment. Significant cyber-attacks affected a number of large UK organisations during May and June 2017, and whilst it is reassuring that the Council’s defence systems were effective with additional patches promptly applied to further increase resilience, it is important not to be complacent as cyber-attacks become more sophisticated and seek to exploit vulnerabilities in networks and security arrangements.

20. Implementation of the new ICT structure saw a new post of Information Security Engineer created and in place to enable a more robust and comprehensive technical analysis of the ICT infrastructure.

21. Steps are also being taken to ensure that all ICT contracts contain references to information security and that they include Cumbria County Council’s expectations especially within the context of reducing the cyber risk to information hosted externally.

22. As part of the agreed 2016-17 audit plan, Internal Audit undertook a risk based review of Cyber Risks. The scope of the Audit between March and June 2017 was to provide independent assurance over management arrangements for ensuring effective governance, risk management and internal controls in the following areas:

- Maintaining Awareness of constantly evolving Cyber Risks.
- Defence Mechanisms against Cyber-Attacks.
- Access Controls
- Policies, Training and Awareness Raising.
- Home Working
- System and Network Monitoring

23. The outcome of the audit provided a ‘Reasonable’ level of assurance. ‘Reasonable’ is defined as “There is a reasonable system of internal control in place which should ensure that system objectives are generally achieved, but some issues have been raised which may result in a degree of risk exposure beyond that which is considered acceptable”.

cumbria.gov.uk
Freedom of Information (FOI)

24. January 2018 marked the 13th anniversary of the introduction of the Freedom of Information Act. During 2017-18, the Council responded to 1306 requests for information under the Freedom of Information Act. This represents a 5% increase compared with 2016-17.

25. The Council responded to 82% (1074) requests within the statutory time limit which represents an improved performance compared with 2016-17 (68%), but remains below the target of 90%.

26. Improved monitoring arrangements have been implemented with Assistant Director level oversight of performance on a monthly basis.

<table>
<thead>
<tr>
<th>Year</th>
<th>Requests received</th>
<th>Requests processed on time</th>
<th>Performance (Target 90%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016/17</td>
<td>1238</td>
<td>844</td>
<td>68%</td>
</tr>
<tr>
<td>2017/18</td>
<td>1306</td>
<td>1074</td>
<td>82%</td>
</tr>
</tbody>
</table>

Environmental Information Regulations (EIR)

27. During 2017-18 the Council received the lowest annual number of requests (31) for information under the Environmental Information Regulations to date, with a 77% decrease compared to 2016-17.

28. As in previous years, the Economy and Highways Directorate received the highest number of EIR requests during 2017-18, due mainly to the services covered by the Directorate such as planning, highways and waste management.

29. The majority of EIR requests received in 2016-17 were from the same applicant and related to CON29/Highways Searches/Land Charges. The request handling process was reviewed mid-year by the Information Governance Team in consultation with the Searches Team and this has improved efficiency of the process. A performance summary compared with 2016-17 is shown below:-

<table>
<thead>
<tr>
<th>Year</th>
<th>Requests received</th>
<th>Requests processed on time</th>
<th>Performance (Target 90%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016/17</td>
<td>136</td>
<td>69</td>
<td>51%</td>
</tr>
<tr>
<td>2017/18</td>
<td>31</td>
<td>24</td>
<td>74%</td>
</tr>
</tbody>
</table>

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

30. 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 two years the council has handled the following requests with performance shown against the target to process 90% within 40 days.

<table>
<thead>
<tr>
<th>Year</th>
<th>Requests Received</th>
<th>Requests processed within 40 Days (Number)</th>
<th>Requests processed within 40 Days (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016-17</td>
<td>191</td>
<td>126</td>
<td>66%</td>
</tr>
<tr>
<td>2017-18</td>
<td>157</td>
<td>101</td>
<td>64%</td>
</tr>
</tbody>
</table>

31. The Information Governance Team receives and allocates requests for social care, education and other data, whilst the Service Centre handle requests for personnel data directly.

32. During 2017-18 performance dipped during Quarter 1 due to the post of SAR Officer being vacant for a period. A new post holder has been in place since June 2017 with enhanced software implemented in November 2017 to allow for processing efficiencies in the handling of requests. This has seen a continual improvement in performance with Quarter 4 showing 71% of requests processed within 40 days. Further development work is scheduled to increase the number of staff able to undertake this role as the implementation of GDPR has resulted in a reduced response time of “one month” in responding to requests as opposed to the previous 40 day target.
Internal Reviews

33. Customers who submit a FOI or EIR 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 2017-18, the Council has processed the following Internal Reviews:

<table>
<thead>
<tr>
<th></th>
<th>2016-17</th>
<th>2017-18</th>
</tr>
</thead>
<tbody>
<tr>
<td>Freedom of Information</td>
<td>36</td>
<td>32</td>
</tr>
<tr>
<td>Environmental Information Regulations</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Data Protection Act</td>
<td>5</td>
<td>5</td>
</tr>
</tbody>
</table>

Referrals to the Information Commissioner’s Office (ICO)

34. 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.

35. 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 2017-18 the Council were notified of the following referrals to the Information Commissioner:

<table>
<thead>
<tr>
<th></th>
<th>2016-17</th>
<th>2017-18</th>
</tr>
</thead>
<tbody>
<tr>
<td>Freedom of Information</td>
<td>13</td>
<td>8</td>
</tr>
<tr>
<td>Environmental Information Regulations</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>Data Protection Act</td>
<td>2</td>
<td>9</td>
</tr>
</tbody>
</table>

36. 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. Three decision notices were issued by the ICO to the Council during 2017-18. In two of these cases the ICO decision was not to uphold the complaint finding the Council had acted correctly in applying exemptions to the release of information. However in one case the Council was found to have breached the timescales for responding. As the response had since been provided the Commissioner required no further action.

Referrals to the First Tier Tribunal (FTT)

37. 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 Government, 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.

38. During 2017-18 the Council received the following referrals to the First Tier Tribunal:

<table>
<thead>
<tr>
<th></th>
<th>2017-18</th>
<th>Outcome</th>
</tr>
</thead>
<tbody>
<tr>
<td>Freedom of Information</td>
<td>1</td>
<td>Decision Awaited</td>
</tr>
<tr>
<td>Environmental Information Regulations</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Data Protection Act</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>
Charges

39. 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. The Council will only charge for disbursements in excess of £5. 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 2017-18 the Council did not issue any fee notices as all disclosures were provided by e-mail with relevant information attached if required.

Exemptions

40. 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.

41. 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).

42. 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.

43. During 2017-18 the Council applied an exemption to 90 requests and the breakdown for type of exemption and times applied is presented below.

<table>
<thead>
<tr>
<th>Exemption</th>
<th>Times Applied</th>
</tr>
</thead>
<tbody>
<tr>
<td>Section 09 – Fee Notice</td>
<td>6</td>
</tr>
<tr>
<td>Section 12 - Exceeds Cost Limit</td>
<td>27</td>
</tr>
<tr>
<td>Section 14 - Vexatious or Repeated</td>
<td>4</td>
</tr>
<tr>
<td>Section 21 – Reasonably Accessible by other means</td>
<td>23</td>
</tr>
<tr>
<td>Section 22 - Future Publication</td>
<td>2</td>
</tr>
<tr>
<td>Section 23/24 – Security Bodies / National Security</td>
<td>1</td>
</tr>
<tr>
<td>Section 30- Environmental Information</td>
<td>1</td>
</tr>
<tr>
<td>Section 31 – Law Enforcement</td>
<td>5</td>
</tr>
<tr>
<td>Section 39 – Environmental Information</td>
<td>1</td>
</tr>
<tr>
<td>Section 40 – Personal Data</td>
<td>10</td>
</tr>
<tr>
<td>Section 41 – Confidentiality</td>
<td>1</td>
</tr>
<tr>
<td>Section 42 – Legally Privileged</td>
<td>1</td>
</tr>
<tr>
<td>Section 43 – Commercially Sensitive</td>
<td>7</td>
</tr>
<tr>
<td>Section 44 – Prohibitions on Disclosure</td>
<td>1</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>90</strong></td>
</tr>
</tbody>
</table>

Service Costs

44. 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.
45. 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.

<table>
<thead>
<tr>
<th></th>
<th>2015-16</th>
<th>2016-17</th>
<th>2017-18</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Number of Requests</td>
<td>1379</td>
<td>1374</td>
<td>1337</td>
</tr>
<tr>
<td>Estimated Cost of processing requests in Directorates.</td>
<td>£213,000</td>
<td>£186,273</td>
<td>£199,175</td>
</tr>
<tr>
<td>Cost of the central team</td>
<td>£103,000</td>
<td>£103,639</td>
<td>£102,111</td>
</tr>
<tr>
<td>Total estimated cost</td>
<td>£316,000</td>
<td>£289,883</td>
<td>£301,286</td>
</tr>
<tr>
<td>FTE in Central Team</td>
<td>2.5</td>
<td>2.4</td>
<td>2.5</td>
</tr>
<tr>
<td>Estimated unit cost per request</td>
<td>£229</td>
<td>£221</td>
<td>£226</td>
</tr>
<tr>
<td>ICO threshold for refusal per request</td>
<td>£450</td>
<td>£450</td>
<td>£450</td>
</tr>
</tbody>
</table>

Transparency and Open Data

46. 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.

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


48. During 2017-18, there have been a number of notable achievements in this area:

- a consistent approach to the publication of the Council’s organisational structure;
- design, maintenance and publication of a disclosure log.

Action Plan for 2018/19

49. The following additional actions are to be incorporated into its Corporate Governance Action Plan for 2018/19:

- **Delivery and roll out of a new data breach incident reporting tool.**
  A new on-line reporting tool has been developed to allow data breaches to be reported in a more efficient manner as well as capturing full details of an incident to allow for assessment to be made at the point of receipt as to whether a self-referral to the ICO is required.

- **Creation of an Information Governance Performance Dashboard.**
  To provide a regular visual view as to performance being achieved.

- **To raise the profile and capacity to increase prioritisation of: FOIs, EIRs, Subject Access Requests and to create a learning culture from data breaches.**

- **Achieving performance targets for processing FOI, EIR & SAR requests within statutory timescales.**
  Performance reports are now being produced on a weekly basis with regard to FOI response performance which also highlights cases that are reaching their statutory response deadline of 20 working days. Directorate Management Teams also review performance reports on a monthly basis.

- **Embed GDPR requirements in the new council culture.**
  A series of communications and training has been created to inform staff as to GDPR requirements as well as the creation of a mandatory E-Learning module. A review and updating of Privacy Notices has taken place to ensure our customers are made aware of how we intend to use the data they provide.

- **Information Governance Training & Information Security Training:**
  Corporate Governance Group have a standing agenda item to consider the Council’s performance in meeting its target of 95% of staff having undertaken the GDPR and Information Security Training on an annual basis. Part 2 of the Information Governance Training for Senior Managers will continue to be rolled out.
Conclusion

51. In summary, progress has been made during 2017-18 with key actions taken to strengthen the Council’s approach to effectively manage information risks and ensure a robust approach to information governance.

52. There will always be room for continual improvement, and information governance and data security will remain a corporate priority during 2018-19 and it is important to maintain a corporate focus and ensure resources remain committed to this important agenda.

53. In particular, as the potential for cyber risk increases, it is essential the Council takes action to understand and mitigate risk in this area; as well as ensuring it complies with changing legislation and requirements in particular in ensuring it complies with the GDPR requirements.

54. The Council requires ongoing focus to ensure data is secured and processed appropriately to minimise and reduce any data breaches or near misses, with learning and awareness raising a key corporate priority.

Dawn Roberts
Executive Director – Corporate, Customer and Community Services

Further Information

For further information and guidance please contact:

Steve Tweedie
Information Governance and Risk Manager
Information Governance Team | Resources and Transformation
Cumbria County Council | Cumbria House | 117 Botchergate | Carlisle | CA1 1RD
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.

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 diliinizde görmek istiyorsanız lütfen 01228 606060 numaralı telefonu arayınız

Cumbria.gov.uk