Doncaster
Metropolitan Borough Council

Agenda Item No. 6
4th February, 2015

To the Chair and Members of the
AUDIT COMMITTEE

INFORMATION GOVERNANCE PROGRESS REPORT

EXECUTIVE SUMMARY

1. The purpose of this report is to inform the committee of the Council's position before a Senior Information Risk Owner (SIRO) and Customer Information Team (consisting of Data Protection, Freedom of Information, Information and Records Management and Complaints functions) were appointed. It also sets out what these roles have achieved and coordinated for the authority including actions to protect the Council in the past from:

- Potential action from the ICO due to concerns around how the Council managed its adherence to the Freedom of Information (FOI) Act 2000.

- A potential fine from the Information Commissioner's Office (ICO) potentially up to 500k, due to concerns resulting from perceived insufficient measures to ensure the Council managed its adherence to the Data Protection Act 1998.

- A potentially unacceptable rating and resulting measures from the ICO in relation to the perception that the Council was potentially not meeting its legal obligations with regard to information governance.

2. It also includes that these roles have not only been responsible for deterring the above but have also ensured the Council:

- Meets all it legal obligations with regard to information governance and continues to improve.

- Achieves a high response rate within statutory timescales for FOI requests, Local Government Ombudsman (LGO) enquiries, complaints and data protection subject access requests.

- Has greatly reduced the number of data protection breaches for the Council with only one in quarter 3 of this financial year.

- Has improved the Council's rating with the ICO with regard to information governance by completing urgent actions for the Council to obtain a 'Limited Assurance' rating and then by implementing

recommended actions to achieve a 'Reasonable Assurance' rating with no further audit planned.

3. Further to this, it details the key actions still being progressed by the team and future objectives such as:

- The implementation of one record store for the Council in line with the Council's asset rationalisation agenda.
- Ensuring the Children's Trust operates within the required information governance requirements for the Council.
- The introduction of automated and efficient data archiving, retention and disposal.
- The reduction of paper records in line with implementing a digital council.
- Introduce and maintain data governance for the soon to be introduced single customer record, one of the capabilities being developed for the organisation by the Digital Council Programme.
- Involvement in the proposed single business intelligence store for the authority as agreed in the Council's ICT Strategy.
- On-going involvement in ensuring the Council meets its data security requirements for Public Services Network compliance.
- Also of course, not forgetting the key work that must continue on a daily basis to ensure all governance mentioned above and now in place is maintained.

EXEMPT REPORT

4. Not applicable.

RECOMMENDATIONS

5. Members should note and comment on the content of this report.

WHAT DOES THIS MEAN FOR THE CITIZENS OF DONCASTER?

6. The embedding of robust information governance policies and procedures ensures that the Council adequately protects its citizen's information, minimises the risk of this information being compromised and is open and transparent on how public money is spent. The effective complaint procedure in place informs our customers that we are committed to dealing with all complaints fairly and impartially, and to provide high quality services to all of our customers.

BACKGROUND

7. The statutory Senior Information Risk Owner (SIRO) for the Council and the Customer Information Team within Customer Services are responsible for ensuring that the Council adheres to legislation, policy and procedure relating to:

- Data Protection;
- Freedom of Information;
- Information Management;
- Records Management;
- Local Government Ombudsman enquiries; and
- Complaints.

8. Before the SIRO and Customer Information Team were appointed:

- The Council had no Information Governance function. Information Governance is a framework made up of a set of policies and procedures that set out the rules, roles and responsibilities of staff and compliance measures of how organisations manage their information. Information governance covers all areas of information security, information management, records management, data protection and freedom of information procedures. Without these rules the Council is at risk of not meeting its statutory obligations relating to information governance.

- Although there was a Data Protection Officer and a Freedom of Information Officer, they did not sit in the same team therefore did not work as effectively as possible. Other roles key to the achievement of the organisations obligations with regard to information governance did not exist. There was no reporting or investigation mechanism for breaches of the Data Protection Act. Although there was a Data Protection Officer in post, often they would only become aware of Data Protection breaches following contact from the ICO.
- The Council did not have the mandated roles relating to information governance in place. These are:

- Accounting Officer - The Accounting Officer has overall responsibility for ensuring that information risks are assessed and mitigated to an acceptable level. Information risks must be handled in a similar manner to other major risks such as financial, legal and reputation risks.
- Senior Information Risk Owner (SIRO) - The SIRO is an executive who will implement and lead the risk assessment and management processes within the organisation and advise on the effectiveness of information risk management across the organisation. The SIRO takes ownership of the organisations risk policy and acts as an advocate for information risk.
- Information Asset Owner - IAO's are senior officers who are involved in the management of the service and are able to make decisions concerning the information assets.
- Information Asset Administrator - IAA's ensure that policies and procedures are followed, recognise actual or potential security incidents/threats, consult

their IAO on incident management and ensure that information asset registers are accurate and up to date.

- Business System Owner - BSO's are responsible for administering systems that store information.

- Without these roles the Council was unable to maintain the appropriate protection of information assets.

- As well as the above mentioned roles, the Council did not have in place an Information Governance Board, having responsibility for implementing and embedding information governance within the Council. Providing advice and assurance and decisions on all matters concerning records management and information management with representatives from the whole organisation.

- The Council did not have an embedded Data Retention and Disposal Policy or Data Retention Schedule in place which is required under the Freedom of Information Act. Having a clear policy ensures that legislative obligations are adhered to by introducing mandatory roles and procedures that are standardised across the whole authority. Embedding a Data Retention Policy enables the Council to deliver effective and efficient services by alleviating the need to keep information longer than necessary whilst retaining records vital to service delivery. A Data Retention Policy ensures customers understand what information the Council holds and how long the information is retained for according to legislation and business need.

- The Council did not have a centralised records management function. Records were stored in various locations with many records being stored insecurely in team areas across the borough. Many years ago teams began storing some records at a private facility in Thorne and some records were moved to the Archives facility in Balby. Following the move to the Civic Offices many vacated premises were left with thousands of documents containing personal and sensitive information. This meant that information was difficult to find, kept for longer than it should be kept and at risk of loss, theft or accidental destruction, all of which can incur a large fine from the ICO.

9. Further to this, the Freedom of Information function had previously undergone an audit by the Information Commissioners Office (ICO) that oversee compliance with the Data Protection Act 1998 and the Freedom of Information Act 2000.The issues identified at the time were:

- Responses falling outside the statutory 20 working day timescale with no communication with the customer.

- Inaccurate use of exemptions; refusal of FOI requests not meeting the requirements of section 17 of the Act; this resulted in an increase in the number of appeals received and complaints to the ICO.

- ‘Piecemeal’ disclosure and withholding of information – the ICO raised concerns regarding the Councils records management procedures in some cases.

  The Council had also signed an undertaking with the ICO in 2011, due to two breaches of the Data Protection Act. The undertaking dictated that the Council must make improvements in relation to information security and that appropriate technical and organisational measures would be taken to ensure against the unauthorised or unlawful processing of personal data and against accidental loss, destruction of or damage to personal data. *It should be noted that the ICO can impose a fine of up to £500,000 for none compliance with information governance.*

10. To put things right, the SIRO and the Customer Information Team have completed or ensured the following:

- The roles of the Information Management Officer, Records Management Officer and Records Management Assistant roles have been established and sit in the Customer Information team with the Data Protection Officer, the Freedom of Information Officer and the Complaints Officer, managed by the Customer Information Manager.

- The mandated roles relating to Information Governance have been implemented across the organisation. The Chief Executive is the Accounting Officer, the Director of Finance and Corporate Services is the SIRO and the Heads of Service are the IAOs. The IAO’s have nominated from their service areas, IAAs and BSOs. Specific training has been developed and delivered to these individuals to ensure they are aware of their obligations in these roles.

- The SIRO Information Governance Board (SIGB) has been established with representation across the organisation and key decisions are made by this board. Since its establishment the Board has made amongst others, the following decisions/processes that were previously not considered to be assessed by information governance experts:
-
  - All Data Sharing requests presented to the board and determined.

  - Un-encrypted laptops are a very high information governance risk as they are easily stolen or accessed by other parties. The ICO are able to levy fines if personal information is lost because of this. The board therefore made the decision to encrypt all laptops.

  - Instigated investigations into alternative ways of working where there is a requirement to send documents with personal information to a large number of both internal and external recipients. The outcome being that a technical solution has been introduced.

  - Following the decommissioning of Council premises, many documents containing personal information were found to be abandoned. The

SIGB have implemented a process where vacant premises are assessed prior to the decant process being signed off.

- The SIGB made the decision to procure a software solution called Active Navigation to review all the data held on the s: drive. The council has identified over 15 million files. Although the numbers of files stored continues to increase year on year very little effort is put into deleting any files. The product scans the network and identifies file information such as age of the file, the contents of the file and using the inbuilt reporting tools allows this unmanaged data to be managed. The software can initially identify ROT (redundant, obsolete and trivial) files such as backup or temporary. By analysing the contents of the files the software determines all the duplicate copies of a file with a view to deleting or re-organising folders on the shared network to potentially reduce the files stored. The Customer Information Team has started to delete unnecessarily held data in line with data retention legal obligations.
-
- Developed and implemented the relevant policies and procedures relating to Information governance. This includes:
  - An Information Governance Strategy;
  - An Information and Records Management Policy;
  - A Records Transfer Procedure; and
  - A Data Retention and Disposal policy.

- The Council needed to address the issue of paper records management particularly with the move to the Civic Office as storage space is limited. The Customer Information Team has implemented the categorisation of Hot, Warm and Cold storage to enable teams to store their records based on the frequency of access required. A town centre records store is now in place storing over 6,000 boxes of Council records. Procedures have been implemented for the storage, retrieval, transfer and destruction of records stored. This facility also manages the deeds store and the Legal Child Care Teams records.

- Following on from the implementation of the Data Protection breach investigation process, the number of breaches reported has reduced significantly. The table below details the number of Data Protection breaches reported in the previous financial years. In 2014/15 there has been 24 received up to 31/12/14 and this has reduced significantly in the last quarter.

Year	Number received
2012/13	44
2013/14	58

- The Customer Information Team appointed Freedom of Information Lead Officers in each service area to work with the Freedom of Information Officer ensuring appropriate responses are provided to requests and appeals in accordance with the Act. A process has been put in place which provides clear direction for the appropriate handling of requests. The response timescales are of a high percentage particularly given the large amount of requests the Council receives and the complexity of some of the requests. The number of complaints considered by the Information Commissioner since the audit is also considered to be low. The table below details the number Freedom of Information requests received in the previous financial years. In 2014/15 there has been 952 received up to 31/12/14.

Year	Number received	% responded to in 20 working day timescale
2012/13	943	97.4%
2013/14	1,393	96.5%

11. Whilst all this work was being progressed the ICO contacted us regarding a consensual audit. In 2012 they performed the audit in order to assess the organisations processing of personal data under the Data Protection Act 1998. The Council agreed to this and auditors carried out a 3 day inspection. The audit scope was limited to Adults Social Care (Safeguarding), Human Resources and Revenues and Benefits and specifically looked at:

- Training and awareness – the provision and monitoring of staff data protection training and awareness of data protection requirements relating to their roles and responsibilities.

- Records management – the processes in place for managing both electronic and manual records containing personal data, including the controls in place to monitor the creation, maintenance, storage, movement, retention and destruction of personal data records.

- Information Sharing – the design and operation of controls to ensure the sharing of personal data complies with the principles of the Data Protection Act 1998 and the good proactive recommendations set out in the ICO's Data Sharing Protocols.

Following on from the ICO audit, the Council received the final report from the ICO on the 8th February 2013 and the ICO's overall assessment of the Council was 'Limited Assurance'. This meant that the arrangements for data protection compliance with regard to governance and controls provided only limited assurance that processes and procedures were in place and were being adhered to. The audit identified scope for improvement in the then existing arrangements by providing 34 recommendations. The assessment for Training and Awareness was 'reasonable assurance', but for both Records

Management and Information Sharing the assessment was 'limited assurance', therefore the overall assessment was 'limited assurance'. 6 recommendations were made relating to Training and Awareness, 20 recommendations were made relating Records Management and 8 recommendations were made relating to Information Sharing.

- **Training and Awareness summary** – The Information Governance roles and responsibilities needed to be formalised across the Council. An annual Data Protection training plan needed to be developed, detailing mandatory training specific to an employee's role in the organisation, refresher training, reporting of training statistics and the monitoring and escalation of mandatory training not completed.

- **Records Management summary** – The Council needed to ensure that an appropriate records management governance framework was defined and key personnel identified to be responsible for records management strategy, policy, operations and compliance monitoring. The recently introduced structure of Information Asset Owners needed to be embedded across the council and the further identification of the Information Asset Administrators and Business System Owners was recommended. Recommendations were made relating to the storage of paper records, the security of these records and the monitoring of records following their temporary removal from storage.

- **Data Sharing summary** – The Council needed to develop a Data Sharing protocol to regulate data sharing with partners. The data sharing protocol should identify an officer responsible for data sharing agreements and their review, including a central log of all data sharing agreements.

The outcome of the ICO consensual audit determined any follow up action that the ICO would take. As the Councils overall assessment was limited, the ICO would conduct an email follow up at six months and determine whether a follow up visit was required. The email follow up was completed in October 2013 with the Council submitting a questionnaire and additional documents to evidence the work undertaken to ensure achievement of the recommendations. In December 2013 the Council received the follow up report from the ICO and the overall assessment had increased to 'reasonable assurance'. All of the recommendations have been completed or are ongoing.

12. Moving forward, the SIRO and Customer Information Team will:

- Continue to ensure the recommendations from the ICO audit are adhered to;

- Continue to ensure that the organisation meets its statutory obligations relating to information governance;

- Continue to embed information governance policies across the organisation;

- Continue to ensure that requests for information under the Freedom of Information Act are responded to in timescale and the appropriate information is supplied giving consideration to the exemptions within the Act;

- Continue to deal with Subject Access Requests for information under the Data Protection Act, ensuring that the redacting is completed to ensure that only the appropriate information is released to the requester;

- Continue to provide advice on the security of information and carry out the necessary investigation when a breach of Data Protection may have occurred;

- Continue to ensure each member of staff and elected member is aware of their responsibilities relating to information governance by delivering training and providing guidance and advice;

- Undertake a comprehensive review of the current records management stores in the Town Centre, at Thorne and at Balby, and implement a new Council wide records management solution by identifying suitable Council premises or alternative solution to house the 26,000 boxes of Council records;

- Continue to destroy the paper records stored according to the Data Retention and Disposal Policy;

- Further improve how electronic data is managed initially by reviewing the data held using Active Navigation and deleting the ROT;

- Continue to ensure the Council responds within timescale and effectively to complaints raised about services provided by or on behalf of the Council;

- Continue to ensure that the organisation investigates and responds within timescale to enquiries made by the Local Government Ombudsman about services provided by or on behalf of the Council;

- Ensure any records are removed from other council buildings across the borough and include in the one record store for the Council in line with the Council's asset rationalisation agenda;

- Ensure the Children's Trust operates within the required information governance requirements for the Council;

- The introduction of automated and efficient data archiving, retention and disposal;

- The reduction of paper records in line with implementing a digital council;

- Introduce and maintain data governance for the soon to be introduced single customer record, one of the capabilities being developed for the organisation by the Digital Council Programme; and

- Involvement in the proposed single business intelligence store for the authority as agreed in the Council's ICT Strategy.

OPTIONS CONSIDERED

13. Not applicable

REASONS FOR RECOMMENDED OPTION

14. Not applicable

IMPACT ON THE COUNCIL'S KEY PRIORITIES

15.

Priority	Implications
We will support a strong economy where businesses can locate, grow and employ local people. • *Mayoral Priority: Creating Jobs and Housing* • *Mayoral Priority: Be a strong voice for our veterans* • *Mayoral Priority: Protecting Doncaster's vital services*	**1.** The embedding of robust information management arrangements within the Council contributes to the effective delivery of all the Council's key priorities
We will help people to live safe, healthy, active and independent lives. • *Mayoral Priority:* Safeguarding our Communities • *Mayoral Priority:* Bringing down the cost of living	
We will make Doncaster a better place to live, with cleaner, more sustainable communities. • *Mayoral Priority: Creating Jobs and Housing* • *Mayoral Priority: Safeguarding our Communities* • *Mayoral Priority: Bringing down the cost of living*	
We will support all families to thrive. • *Mayoral Priority: Protecting Doncaster's vital services*	
We will deliver modern value for money services.	
We will provide strong leadership and governance, working in partnership.	

RISKS AND ASSUMPTIONS

16. There are many risks associated with on-going information governance, the main ones being:

- Potential breaches in data protection;
- Continuous technical threats to data security and digital information; and
- Ensuring secure and appropriate storage of paper documentation.
- These risks are taken very seriously by the Council and mitigated against 24/7 365 days a year.

LEGAL IMPLICATIONS

17. The implementation of the recommendations of the ICO audit and the measures highlighted in the report to ensure continued compliance will ensure that the Council continues to meet its obligations in relation to information governance. Failure to comply with these obligations could lead to enforcement action, which can include the imposition of substantial fines by the Information Commissioner**,** compensation claims from individuals, as well as consequential reputational damage to the Council.

FINANCIAL IMPLICATIONS

18. Should any specific initiatives be required, in response to the management of information risks, any cost implications will be reported and addressed as and when they arise. The ICO can impose fines of up to £500,000 for none compliance with Information Governance legislation.

HUMAN RESOURCES IMPLICATIONS

19. Not applicable.

TECHNOLOGY IMPLICATIONS

20. Should any technology issues or requirements arise, these will be submitted to the ICT Governance Board for consideration.

EQUALITY IMPLICATIONS

21. Decision makers must consider the Council's duties under the Public Sector Equality Duty at s149 of the Equality Act 2010. The duty requires the Council, when exercising its functions, to have 'due regard' to the need to eliminate discrimination, harassment and victimisation and other conduct prohibited under the act, and to advance equality of opportunity and foster good relations between those who share a 'protected characteristic' and those who do not share that protected characteristic. There are no specific equality implications arising from this report. However, any activities arising from the management of information will need to be the subject of separate 'due regard' assessments.

CONSULTATION

22. There are no specific consultation requirements, however many stakeholders have been involved in this process and will continue to be on an on-going basis.

BACKGROUND PAPERS

23. None.

AUTHORS & CONTRIBUTORS

Sarah Marshall
Customer Information Manager
Tel 01302 862547
Sarah.Marshall@doncaster.gov.uk

Julie Grant
Assistant Director, Customer Services & ICT
Tel 01302 862496
Julie.grant@doncaster.gov.uk

Simon Wiles

Director of Finance & Corporate Services