

Joint Report of the Director of Customer & Business Support Services,
and the Head of Internal Audit (Veritau)

Information Governance Strategy Update, Including Freedom of Information Processes

Summary

1. Security of data and compliance with the Data Protection Act have become increasingly important to the council and to other local government bodies. The Audit and Governance Committee approved a strategy in 2011 to bring the council into compliance with good practice in this area. This paper summarises progress to date and highlights the key areas remaining to be addressed.
2. This report briefly updates members on information governance developments including Data Protection (DP) and Freedom of Information (FOI) matters. This will assist members in monitoring risk areas highlighted in the council's Annual Governance Statement.

Background

Data Protection and Information Governance

3. Earlier this year, the Information Commissioner and the Chair of the Local Government Association wrote jointly to all Council Leaders reminding them of their legal obligations in regard to Data Protection. The letter reminded local authorities that the ICO had levied monetary penalties of over £1.5m on local authorities since 2010 and pointed to an increased focus by the ICO on compliance by local government in their investigations.
4. In the last three years, the council has been the subject of several investigations by the ICO following reports of data breaches. Apart from the investigation in 2010 which resulted in the council being required to sign an undertaking to comply with the Data

Protection Act, the ICO have thus far been satisfied with the action taken by the council in more recent cases.

Breaches

5. A number of other public bodies and service providers have been subject to enforcement action by the ICO in the last year. Recent cases have included the following:
 - **North East Lincolnshire** - hundreds of children's details were lost on an unencrypted council memory stick (this incident resulted in a £80,000 fine)
 - **NI Department of Justice** – the ICO levied a £185,000 penalty after a filing cabinet containing details of a terrorist incident was sold at auction
 - **The British Pregnancy Advice Service (BPAS)** – the ICO levied a £200,000 fine after thousands of people's personal details were revealed to a malicious hacker
 - **A Welsh home care provider** - the files of 10 vulnerable and elderly people were found on a street in Neath Port Talbot
 - **Kent Police** – the ICO levied a £100,000 fine after confidential information, including copies of police interview tapes, was left in the basement of a former police station.
6. In addition to the above, Basingstoke and Dean Borough Council have recently reported a breach in which the details of 1,900 benefit claimants were inadvertently disclosed in response to a Freedom of Information request. This happened when a spreadsheet sent in response to the Fol enquiry was found also to contain detailed source information (names, addresses etc). This incident repeats previous cases elsewhere where spreadsheets containing pivot tables have been sent out inadvertently in response to Fol enquiries.
7. Within the council, there is an established system for reporting data breaches. Since April 2013, 38 such cases have been reported. Most of these were found to be the result of human error and affected small numbers of people. However, one recent breach resulted in the personal email addresses of a large number of correspondents (in relation to Lendal Bridge) being widely circulated. This incident is currently subject to an ICO investigation.

Legal Requirements and CYC Strategy

8. In March 2011, CYC approved a long term strategy for the council to meet its legal obligations in terms of Information Governance. The strategy aimed to ensure compliance with the Cabinet Office Information Assurance Maturity Model (IAMM) level 1 by March 2015. The attached document at Annex A shows progress made against the main deliverables in that strategy.
9. Apart from the strategy, experience has shown that, when a data breach occurs, the ICO looks for evidence that the organisation can demonstrate that a number of key elements are in place. In summary, these are:
 - Demonstrable top level commitment (eg. CMT involvement and Audit and Governance Committee oversight)
 - Clear, effectively communicated and enforced policies
 - Effective physical security and IT controls
 - Staff training and evidence that staff have understood the key policies
 - A comprehensive and clearly communicated breach reporting and investigation system
 - Feedback and a lessons learnt culture; and
 - Disciplinary action being taken in cases of data breaches where members of staff have failed to comply with policies.

Progress against the strategy

10. Overall, the council has made significant progress in meeting level 1 of the IAMM. Further details are provided in Annex A, but the key recent developments have been:
 - The implementation of a new software application (icomply) to enable the provision of an information governance e-learning facility. More work is required to develop the training packages, but the delivery method is now in place and this will provide evidence that staff have received training and have understood the contents. Whilst this software was specifically acquired for use in Information Governance training, it has the potential for much wider application.
 - Encryption of laptops and removable devices is a key control to prevent inadvertent data loss. Failures in this area have been a

consistent feature in cases elsewhere which have resulted in fines being levied by the ICO. The council routinely issues encrypted laptops and detachable storage devices, however more work is needed to ensure that all laptops and devices can be located and responsibility for them clearly assigned

- Mobile devices and the risk surrounding them are becoming increasingly important. The council has installed the facility to locate, restrict e mail access and remotely wipe mobile devices. ICT are able to initiate the remote location and wipe facility, thus preventing unauthorised access to sensitive data.
11. A data breach reporting system is also now in place. However compliance with this is variable with some directorates reporting breaches and others reporting many less than would be expected given the nature of their work. Training through icomply can be expected to increase staff awareness and understanding of the importance of breach reporting, however to be most effective managers will need to re-enforce these messages with their teams.

Freedom of Information (FOI) Requests

12. At the meeting of this committee on 26th September 2013, members learned more about the council's review of FOI processes to respond to the draft Annual Governance Statement, including information governance risks around the processing of FOIs and also on the planned improvements to meet the recommendations from the internal audit review.
13. Since commencing a centralised approach the total amount of business passing through the Customer Feedback Team has risen by 400%, the majority is related with complaints but with an evident increase in number of FOIs received.
14. During 2013/14 overall 81% of FOIs were answered within the 20 day prescribed deadline set by the Freedom of Information Act 2000. The council has received a 72% increase in the number of FOI enquiries in 2013/14 (1384) from the number received in 2011/12 (804).
15. According to a survey of councils carried out by University College London (UCL) in 2010, the average percentage of requests completed by unitary authorities within 20 days was 83.2%.

16. It is important to note however that following the changes to FOI processes and the introduction of improved monitoring processes, which was described at the meeting on 26th September 2013, there has been significant improvement in the % of FOI enquiries responded to in time as shown in the table below.

| | Oct | Nov | Dec | Jan | Feb | Mar |
|------------------------|-------|-------|-------|-------|-------|-------|
| Percentage In Time | 99.2% | 97.3% | 90.6% | 99.4% | 95.6% | 90.3% |
| Percentage Out of Time | 0.8% | 2.7% | 9.4% | 0.6% | 4.4% | 9.7% |

NB In future a rolling graph will be included to show monthly figures including trends

17. The number and nature of FOIs, however continue to increase in number and complexity. Annex B shows the FOIs received into the council in one week ending 13 June 2014.
18. The intention is to achieve performance to exceed 95%. Work will also be done to try and increase the amount of information on the website and to target enquiries to this information where relevant.

Review of Fol requests

19. Following discussions with the ICO, the council has introduced a system of independent review for cases where customers are unhappy with the response to Fol requests. In order to maintain a clear separation and demonstrate the independence of these reviews, they are carried out by Veritau. In cases where the request for a review stems from a failure to respond to the Fol request, Veritau seeks to establish the reasons for the delay. In cases where an exemption has been applied, Veritau review the degree to which the exemption has been correctly applied.
20. Over the last year 98 reviews have been carried out. 70 were reviews of the application of exemptions and the remaining 28 of late/non responses. Of the 70 reviews of the application of exemptions, Veritau upheld the council's decision in 43 cases, ruled against the council in 9 and ruled partially in favour of the council in 12 cases. The remaining 6 were withdrawn.
21. In addition to requesting a review through Veritau, dissatisfied customers also have the right of appeal to the ICO. Between April 2013 and March 2014, there were 93 appeals made to the ICO (over half of which were made in the last third of the year). In 40 of those appeals, the ICO found against the council. However, if cases of late/non response are excluded, the pattern changes

significantly, with 48 out of the 58 appeals of substance being found either partially or wholly in favour of the council.

| REASONS FOR REVIEW | ICO Findings | | | |
|----------------------------------|--------------|------------------|---------------------|-------------|
| | Total | In favour of CYC | Partially in favour | Against CYC |
| No response | 31 | 5 | 0 | 26 |
| Response outside 20 working days | 4 | 0 | 0 | 4 |
| Incomplete response | 24 | 18 | 6 | 0 |
| Application of exemption | 27 | 15 | 3 | 9 |
| Information inaccurate | 7 | 6 | 0 | 1 |
| Total | 93 | 44 | 9 | 40 |

Update on the key improvements to FOI processes:

22. In addition to improvements mentioned above, the following changes have been introduced:

- Senders of FOI enquiries made by email are sent an automated email acknowledgment confirming that it has been received and when to expect a response.
- All FOIs are sent to Heads of Service and copied to Assistant Directors.
- The council has introduced the new internal deadline of 15 days at which point a reminder is also escalated to the relevant Assistant Director/Director copied to the Director of Customer and Business Support Services. Any late responses are now required to provide an explanation and assurance to the Director of CBSS.
- There is a clear mechanism in place for cross council enquiries through the Customer Feedback Team.
- Using the guidance available from <https://www.gov.uk/make-a-freedom-of-information-request/how-to-make-an-foi-request> enquirers are asked to provide their name and address where they can be contacted.
- Quarterly quality assurance monitoring conducted by Veritau auditors.

- Following on from the successful achievement of a FOI practitioner qualification for a member of the Customer Feedback Team, training and toolkit information (including a “handy guide to getting it right”) is being developed jointly with Veritau, and will be rolled out to all staff across the council. This will ensure that there are further improvements in the arrangements for determining exemptions early in the process, erroneous and duplicate requests.
- An online FOI enquiry form has been developed and will soon be available through the council website, increasing the contact channels available to make a FOI enquiry.

Update on FOI Monitoring Processes

23. Monthly reports are now made available to Directorate Management Teams including follow up information on out of time responses.
24. Corporate monitoring is being undertaken by the Director of Customer & Business Support Services and the Corporate Information Governance Group (CIGG) as well as annual and interim reports to Audit & Governance Committee, as agreed.
25. Targets were set that would enable CYC to attain the performance levels achieved by the best performing councils as described in the report in September 2013 and progress will be reported against these to members as agreed through six monthly reports to this committee.

Planned further improvements:

26. The following work is planned in this year:
 - Completion of the audit of published data against CYC’s own and nationally prescribed publication schemes, to ensure as much as possible is published in a clear and understandable way, on the council website.
 - This will further inform the changes still needed to be made to improve the transparency and accessibility of such information.
 - CYC will also publish data that is themed to allow easier identification of information which should result in a corresponding reduction in volume of FOI enquiries.

Consultation

27. The report is for information only.

Options

28. The report is for information only.

Analysis

29. All analysis is contained in the report.

Council Plan

30. Data Protection and compliance with the Freedom of Information Act are legal requirements. Failure to adequately safeguard personal data could compromise the Council's relations with partner organisations (eg. the NHS) and make it more difficult to deliver the council's core services. Similarly failure to deliver a good quality Fol service can have reputational damage for the council.

Implications

31. The main implications for the council are reputational, particularly the impact a serious breach of personal data would have on members of the public.

- **Financial** – potential of up to £500,000 penalty levied by the ICO in the event of a serious data breach.
- **Human Resources (HR)** Council wide staff awareness training needs to be implemented (through lcomply) to ensure all staff and members are aware of their obligations and what to do in the event of a breach.
- **Equalities** – None
- **Legal** - a data breach could place the council in contravention of the Data Protection Act and expose the organisation to financial penalties. Implementation of the actions arising from the internal and external reviews of Fol cases will assist in meeting the statutory requirements of the Freedom of Information Act.
- **Crime and Disorder** - none

- **Information Technology (IT)** - medium term system changes are required to integrate FOI, complaints and feedback into the council's Customer Relationship Management System (CRM); this will be built into the IT Development Plan. In regard to Information Security, implications for IT are in terms of compliance with PSN requirements, data retention and IT security.
- **Property** - implications for basic physical security of Council offices.
- **Other - none.**

Risk Management

32. The information, update and actions outlined in this report are intended to reduce the time taken in processing FOIs and publication improvements may reduce the overall number of FOIs received, therefore introducing no new risk. Failing to sustain current performance however will again increase the risk of criticism or intervention from the Information Commissioner which can include financial penalties.
33. Data Protection and Information Security risks are included in the Council's risk registers at several levels.

Recommendations

34. Members are asked to:

- a) Consider and note the Information Governance and Data Protection update.

Reason: To ensure the council meets the requirements of Data Protection legislation, is able to ensure security of key personal data and is able to continue to work effectively with partner organisations.

- b) Consider and note the Freedom of Information update.

Reason: To ensure the council meets the requirements of FOI legislation, and is open and transparent in its publishing of information.

Contact Details

Authors:

Pauline Stuchfield
Assistant Director,
Customers & Employees
Tel: 01904 551100

Max Thomas
Head of Internal Audit
Veritau
Tel: 01904 552940

**Report
Approved**



16-06-14

Specialist Implications Officer(s)

Name Lorraine Lunt
Title Customer Services Support Manager
Tel No 01904 552247.

Name Roman Pronyszyn
Title Client Relationship Manager (Veritau)
Tel No 01609 552284.

Background Papers:

Previous report to Audit & Governance Committee 26 September 2013:
Information Governance Strategy Update, Including Freedom of
Information Processes

Annexes

Annex A - Progress against Level 1 of the IAMM
Annex B – FOIs received weekend ending 13 June 2014.