Corporate Governance and Standards Committee Report

Report of Executive Head of Corporate Development

Author: Vincenzo Ardilio

Tel: 01483 444053

Email: vincenzo.ardilio@guildford.gov.uk

Lead Councillor responsible: Councillor Nigel Manning

Tel: 01252 665999

Email: nigel.manning@guildford.gov.uk

Date: 4 June 2015

Annual report on Guildford Borough Council's compliance with Information Rights legislation

Executive Summary

This is the annual report of the Information Rights Officer to show how the Council has performed in compliance with the Information Rights legislation. In 2014 there was:

- an increase in the number of formal requests for information under the Freedom of Information Act 2000, Environmental Information Regulations 2004 and Data Protection Act 1998 (subject access requests),
- an increase in response timescales in relation to requests made under the Freedom of Information Act 2000 and Environmental Information Regulations 2004 receiving a response outside of the statutory timescales,
- an increase in the number of reported information risk incidents

Recommendation to Audit and Corporate Governance Committee

1. That the committee approves the action to be taken by officers as set out in this report

Reason(s) for Recommendation:
To ensure that the Council continues to improve its compliance with Information Rights legislation so it operates in an open manner whilst providing data privacy for individuals.

1. Purpose of Report

1.1 The Information Rights Officer is required to provide an annual report on the Council's compliance with the Data Protection Act 1998, Freedom of Information Act 2000 and the Environmental Information Regulations 2004 to the Audit and Corporate Governance Committee. These are commonly referred to as the Information Rights legislation.

1.2 This report is for the 2014 calendar year and covers the following areas:

a) formal requests under the Freedom of Information Act (FOI) and the Environmental Information Regulations (EIRs) – a performance and analysis of the management information available;

b) Information Commissioner's Office (ICO) investigations in respect of the above;

c) data protection and privacy, including a summary of reported data protection breaches;

d) Information Rights issues for 2015 and beyond

2. Strategic Framework

2.1. Complying with the Information Rights legislation is consistent with the five fundamental themes set out in the Council's Strategic Framework.

2.2. By promoting openness in the way the Council operates and data privacy for the individuals who use its services, we are able to support society in evolving a self-reliant and sustaining local community, while supporting our most vulnerable residents, who are often the subjects of the most sensitive information the Council holds.

3. Background

Freedom of Information

3.1. Individuals and legal persons have the right to request any recorded information held by or on behalf of the Council. The Council must respond to these requests within 20 working days in all but exceptional cases. In exceptional cases, it may be necessary to extend the response timescale in order to complete a public interest test. Environmental information held by the Council falls under separate, but similar, access rules – namely the Environmental Information Regulations 2004. For ease of reference, requests for environmental information are included with Freedom of Information requests in this report.

Data Protection

3.2. Section 7 of the Data Protection Act 1998 provides any living individual with the right to request their own personal data from the Council. The Council must deal with these requests within 40 calendar days. At the time of writing, we used a separate system (from FOI requests) as they always involve protectively marked information and so we keep them as confidential as our discovery process will allow. During in 2015 we have been implementing a new system for handling both FOI and Subject Access requests.

3.3. Schedule 1, Part 1, Principle 7 of the Data Protection Act 1998 requires us to take appropriate technical and organisational measures against unauthorised or unlawful use of personal data and against accidental loss or destruction of, or damage to, personal data. We have a procedure for staff to report information security risk incidents. The Information Rights Officer reports the outcomes of investigations to

the Executive Head of Organisational Development, who is the Senior Information Risk Owner (SIRO). The Information Rights Officer provides an anonymised summary to the Corporate Governance Group each quarter.

4. Performance with requests for information under the Freedom of Information Act 2000 and Environmental Information Regulations 2004

Table 1 - Freedom of Information (FOI) and Environmental Information Regulations (EIRs) during 2014

	2013	2014	% +/- over prev. year	Comments
Number of formal requests	669	848	27%	This continues the consistent significant increase in the number of requests each year over the last ten years.
Performance (% of requests dealt with within statutory 20 working days)	87%	69%	-18%	Performance did not meet the Information Commissioner's minimum compliance threshold of 85 per cent.
Number of known investigations by the ICO	0	9	Increase	Four individuals were responsible for the nine complaints to the Information Commissioner during 2014. Two complainants made three complaints each, another made two and a fourth made one.

Table 2 – Which Services received requests during 2014

Service involved	TOTAL Number of Requests 2013	TOTAL Number of Requests 2014	2014 Late Responses	% On time
Business Systems	60	69	34	51
Health and Community Care	107	151	67	56
Corporate Development	32	17	6	65
Economic Development	26	26	13	50
Financial Services	21	22	9	59
Housing Advice	40	43	15	65
Human Resources	55	44	6	86
Legal & Democratic	33	31	10	68

Service involved	TOTAL Number of Requests 2013	TOTAL Number of Requests 2014	2014 Late Responses	% On time
Services				
Neighbourhood & Housing Management	28	42	18	57
Operational Services	80	74	41	45
Parks & Leisure	46	74	7	91
Planning Services	76	77	30	61
Revenues & Payment Services	144	188	24	87
Management Team	8	7	4	43
	As some requests involved more than one service, the total of requests in this table will be greater than the actual number of requests received by the Council during the year			

Table 3 – Who made use of the Freedom of Information Act during 2014?

Category selected by officer	No of requests 2013	No of requests 2014
Commercial	176	192
Media	87	83
Charity/interest groups	11	8
Individuals	355	564
Campaign Group	0	1

4.1. Applicants are under no obligation to identify their purpose for making a request under the Freedom of Information legislation. They are simply required to provide a name and address for correspondence. Therefore, it is not always clear whether an applicant is acting in a private capacity, on behalf of an organisation or for other business purposes such as research. However, the current system allows the Council to make a judgment on the capacity in which an applicant appears to be making a request (for example if a company is making a request, an assumption is made that the request is for commercial purposes). It should be noted that this depends on a subjective judgement by the officer logging the request, so the above figures should only be used as a general guide (for example, many journalists submit requests from personal Hotmail and Gmail addresses and such-like, without identifying themselves as journalists and so their requests may be categorised as 'individuals'). Table 3 above shows the data for 2014, bearing in mind the preceding comments.

4.2. We have increased the amount of information published through the transparency page on the website in compliance with the Local Government Transparency Code

2014 and will be keeping the accessibility of the information under review. The following information was published:

Accounts receivable	Debt recovery policy Invoicing
Salaries and benefits	Senior officer salary chart Officers' remuneration Senior staff responsibilities
Service and financial plan	General fund budget book
Invoice payments	Spotlight on our spending
Statement of accounts	Statement of accounts up to the financial year-end 2013/14
Business rates overpaid (credit) accounts	Overpaid credit accounts (published quarterly)
Council-owned land and buildings	Published on OS maps
Energy, greenhouse gas reports	Greenhouse Gas emissions report

5. FOI and EIR referrals to the Information Commissioner's Office (ICO)

5.1. The ICO notified the Council that it was dealing with nine formal appeals in relation to FOI and EIR requests during 2014. This was a significant increase over 2013. However, it should be noted that six of the nine complaints were from two individuals who made three complaints each. A third individual made two complaints.

Year	Known Referrals during 2014	Decisions Against the Council*
2014	9	0
2013*	0	0

* Known at the time of writing

6. DATA PROTECTION AND PRIVACY

Table 5 – Data Protection and Privacy Performance

	2013	**2014**	%+/(-) over 2013
Number of Subject Access Requests:	17	16	-6%
Percentage of requests resolved within 40 days	53%	46%	-7%
Number of these which were appealed to the ICO and investigated	1	0	-100%
Number of security and or confidentiality breach allegations reported to the Information Rights Officer under the information risk incident report procedure	2	9*	+350%
Number of the above, which the Council reported to the ICO	0	2	Increase

Three requests remained on hold at the time of writing. Three of the overdue requests were from a single source and were extremely complex.

*Summaries of these cases are in Table 6

Table 6 – Summary of information risk incidents

	Summary of incident	**Category of incident**	**Resolution**
IRB28	January 2014: The Council sent an anti-social behaviour complaint to the neighbours who had been complained about in error. This resulted in threatening behaviour directed at the complainant.	2 – reportable to the ICO	The Council moved the complainant to alternative accommodation. The risk was incorporated into the Basic Data Protection course for staff The matter was reported to the Information Commissioner's Office (ICO), who stated in Decision Notice ENF0528865: *"In this case, the disclosure appears to be the result of an administrative error by a trained member of staff who through their previous employment, had considerable*

	Summary of incident	Category of incident	Resolution
			experience in dealing with neighbour complaints and a history of dealing with other sensitive matters without any previous incidents of this nature. This would suggest that they were more than qualified to carry out this kind of work, and in this case mistakenly typed the wrong house number in a one off mistake. *"The remedial measures that have been outlined have been noted, and it is expected that these will be fully implemented to prevent reoccurrence. Therefore, the case, as reported to us, does not appear to meet the criteria set out in our Data Protection Regulatory Action Policy necessitating further action by the ICO and is now closed."*
IRB29	Minutes of a 'Team around the family' meeting, containing some sensitive information about one of the family members was sent to an internal "Heritage and Culture" mailing list in error. This was caused by an officer selecting the wrong group suggested by Outlook's auto-complete. There was no disclosure outside of the Council.	0 (Near miss)	The Heritage Manager confirmed that her staff had deleted the email and no further disclosures had occurred. IRO recommended the corporate switch-off of autocomplete, which was not accepted.
IRB30	A member of staff complained that the Council was forwarding all of their emails to their line manager in breach of their privacy. No personal information was disclosed in this instance	0 (Near miss)	No personal data was involved in this instance but the IRO recommended the use of a data guardian pro-forma to ensure managerial intervention in any given instance is necessary and proportionate.

	Summary of incident	Category of incident	Resolution
IRB31	Two officers authorised to access the open revenues system were using the same username and password (the personal log in details of one of the officers).	N/A	This was not an information risk incident as both officers were authorised to access the information but the practice was not compliant with the Acceptable Use of ICT policy. The issue of password sharing is being addressed in general terms through the data protection-training course.
IRB32	Customer reported that she received her rent notification letter together with two notifications relating to three other people in the same envelope. This incident did not involve sensitive personal data. This relates to the daily process by which Housing Benefits and Housing Rents letters are produced separately by the respective services and then matched for enveloping. The separation and enveloping of the letter bundles undertaken in the post room was manual. The number of letters involved and the fact that there were varying numbers of documents for each customer resulted in the likelihood of human errors.	0 (Near miss)	The letters were collected on the day after the matter was reported, so that the incident was contained. Responsibility for the process is now with Revenues and Payment Services. The service provides the documentation to the post-room pre-sorted into the bundles. This means the post room staff need only envelope the documents rather than separate them.

	Summary of incident	Category of incident	Resolution
IRB33	Nineteen credit card receipts misplaced at Electric Theatre. These were the merchant copies, which contain the full 16-digit card number and expiry date of each card. The information at risk did not include names, addresses or CSV numbers. It is debatable whether any personal information, which would allow identification, was disclosed. The incident may have raised questions about PCI compliance, which would have been a matter for audit.	0 (near miss)	No further action was taken in relation to data protection but the matter was investigated by internal audit.
IRB34	July 2014: The Parking Office reported the loss of a credit card receipt containing the card number and expiry date. It was likely that the customer was given both copies. This involved limited information. CCTV was checked but did not provide further insight into the incident.	0 (near miss)	No further action was taken in relation to data protection. Customer notified and advised to inform their bank if they were concerned. The responsible officer anticipated that the new Adelante payment system would reduce the likelihood of similar events happening as the information stored would be more limited.
IRB35	A temporary member of staff based in HR scanned and uploaded two job applications to the JobsGoPublic (JGP) recruitment site but saved them to the incorrect JGP accounts. One applicant viewed her account and saw someone else's application form and raised the issue with JGP and HR. JGP spoke to an HR Advisor, who rectified the matter by saving	1 (Self-contained breach)	HR rectified the error immediately on notification. HR carried out a risk assessment on the process and subsequently changed the procedure so that manual application forms were no longer uploaded.

	Summary of incident	Category of incident	Resolution
	both documents to the correct applicant's accounts.		
IRB36	A package containing, witness statements, bank statements and other personal information about a Housing Options client (potential victim of domestic abuse) was delivered to the Council by recorded delivery but never reached the addressee (who is in the Council's Housing Advice service). The package was never located; though Housing Advice has since reported receipt of some of the contents (some sensitive information remains missing) The receptionist on duty placed the package in the Council's internal post system, which is contrary to the procedure rules. The package should have remained at reception and the addressee notified to collect it in person.	2 (reportable to the ICO)	The receptionist who placed the package in the internal post did not pass the probationary period and no longer works for the Council All reception staff were reminded of the procedures and the consequences of not following them. The office manual was reviewed and the delivery log sheet expanded to include more information so that there is a more complete audit trail. The ICO stated in their closing letter on 26 March 2015: *"We have considered the information you have provided about a potential breach of the DPA and, on the basis of the information we currently hold, we have decided that no further regulatory action is necessary at this stage.* *"This is because the council had training and policies in place to protect personal data. In this instance, the staff member concerned had received training on the handling of postal items, but this training was not followed."*

As noted from Table 6 there was an increase in the number of information risk incidents reported during 2014. It is likely that this is a direct result of the awareness created by the corporate data protection training as well as the implementation of the formal Information Risk Incident Reporting Procedure during 2013.

7. VOLUNTARY AUDIT BY THE INFORMATION COMMISSIONER

7.1. The Council requested an Information Commissioner audit of its records management and subject access request handling in 2013. An update on progress is attached as Appendix 1.

8. Future information rights issues

Freedom of Information and Environmental Information Regulations

8.1. As reported in previous years, the Council put the current system in place for dealing with FOI and EIR requests (and Subject Access Requests) some years ago as a temporary measure and this was being updated at the time of writing. Officers remain eager for the implementation of the Freedom of Information Module, which is part of the Firmstep Customer Relationship Management (CRM) system recently acquired.

8.2. Prioritising the above system will assist with logging and assigning requests and automating the workflow for dealing with them. Officers anticipate that the system will be of great assistance to Executive Heads of Service, who are responsible for ensuring they respond to formal information requests within the statutory response timescales. The new system also promises to provide much more meaningful management reports, which will greatly help in the monitoring of information rights compliance.

Data Protection and Privacy

8.3. The three previous annual reports have commented on the EU General Data Protection Regulation (GDPR), a draft of which was released by the European Commission early in 2014. The GDPR, once agreed, will replace the current data protection laws for EU member states. The draft GDPR was still subject to agreement at the time of writing. The EU Council is slated to reach a decision before the end of 2015.

8.4. The key theme of the proposed GDPR is accountability and the proposals included:

- a single set of data protection rules across the EU,
- abolition of “implied consent”, which would mean consent must be explicitly given in all cases where consent is required
- an obligation to use plain English in privacy statements
- increased responsibility and accountability for those processing personal data
- an obligation to report serious breaches to the ICO within 24 hours
- increased data portability for customers, so that they can transfer their data from one organisation to another more easily
- a “right to erasure” to help people better manage privacy risks, particularly on line

- an obligation for certain organisations to appoint a data protection officer
- potentially bigger fines (based on a percentage of an organisation's annual turnover).

9. Financial Implications

9.1. This report does not propose any additional spending. However, the financial implications of a failure to comply with the Data Protection Act 1998 are considerable. At the time of writing, the ICO may impose a monetary penalty of up to £500,000 for each breach. The new EU regulation proposes penalties of up to 2 per cent of annual turnover.

10. Legal Implications

10.1. The Council's compliance with the information rights legislation has direct legal implications and failure to do so can result in costly enforcement action and compensation claims.

11. Human Resource Implications

11.1. There are no proposals in this report which have any direct human resource implications

12. Conclusion

Freedom of Information and Environmental Information Regulations

12.1. The number of FOI and EIR requests continued to increase for the ninth consecutive year. There has been a notable increase in the number of overdue requests. A replacement of the existing FOI system is urgently required and Executive Heads of Service will need to ensure arrangements are in place in their service to make sure they give priority to responding on time.

12.2. Corporate Management Team now considers a monthly report on response timescales and this is likely to help improve response times.

Data Protection and Privacy

12.3. As with Freedom of Information requests, the Council's 2014 performance of 46% per cent compliance in relation to Subject Access Requests is a decline over 2013. Three of the requests were from a single source and were complex in nature. However, sound records management is at the heart of responding on time to Subject Access Requests (and in fact any formal requests for information) and the Council must still make considerable progress to comply with the ICO audit recommendations. The Council has a legal obligation to manage personal data in a way that promotes compliance with the subject access rights. This is a records management issue, which would need to be prioritised in order to realise improvements in this area of compliance.

13. SUMMARY OF ACTIONS TO BE TAKEN BY OFFICERS

13.1. The basic data protection training course will continue as a means to raise awareness of data protection and information security issues. (Councillor training is also scheduled at the end of June).

13.2. The Firmstep system for dealing with formal requests for information will be implemented during 2015.

13.3. As part of the implementation of the new system, the procedures for dealing with formal requests for information will be reviewed and training-needs identified.

13.4. Corporate Management Team have agreed a local target of 90% of responses to requests within the statutory timescales and now consider a monthly performance report.

13.5. Information governance champions will be appointed in each service to support Executive Heads of Service to ensure requests assigned to them receive a response within the timescales.

13.6. The Senior Information Risk Officer (SIRO) will ensure, through the Information Risk Group that the Council makes further progress with the Information Commissioner's audit recommendations so that there is an improvement in the way the Council handles subject access requests and manages its records.

13.7. Executive Heads of Service will continue to work with the Customer Services Centre and the Executive Head of Organisational Development to improve public access to information and will maintain systems in place to publish non-sensitive information proactively, where there is a clear public interest to do so.

14. RECOMMENDATIONS

14.1. Committee is asked to note the contents of this report and the summary of actions to be taken by officers.

15. BACKGROUND PAPERS

15.1. Guildford Borough Council Data Protection Audit Report Executive Summary October 2013 (available on the Information Commissioner's website)