Committees:	Dates:
Audit and Risk Management Committee	25/06/2013
Subject: Strategic Risk 16: Data Protection Breach	**Public**
Report of: Town Clerk	**For Information**

Summary

The City Corporation routinely manages considerable amounts of personal information. Any failure to manage properly the personal information which we hold, including personal information held by others on our behalf (normally a contractor), is foremost a failure of responsibility to those individuals who are the subject of that personal information, including staff, Members and those to whom we provide our wide range of services.

To highlight the importance of this responsibility, the Information Commissioner has, since 2010, been provided with the power to fine a 'data controller' up to £500,000 for a breach of the Data Protection Act 1998. This is the principal legislation governing the management of personal information. The Commissioner has frequently used this power, particularly in relation to public sector bodies, and is keen to acquire greater auditing powers.

A breach of the Act exposes the City Corporation to reputational, operational and financial consequences.

The gross risk for Strategic Risk 16 is Red, with the likelihood rated as 'Almost Certain' (see Appendix 1). This is because other people's personal information is processed continually by staff, Members, and by third parties on our behalf. The opportunity for error is, therefore, enormous. Processing can range from a small action, such as using a personalised email address, to a large action, such as the relocation to new offices of a paper-based filing system, containing sensitive personal information about children. Processing also occurs throughout the organisation, although the risk is probably greatest in Community and Children's Services.

Mitigating actions include: training and awareness-raising for officers and members; governance arrangements, and IT security measures. Following the promotion of this risk to the Strategic Risk Register, further action will be taken, for example increasing the frequency of reminders to staff.

This report explains the structure of responsibility within which the risk is managed, as well as associated actions which have brought the net risk to Amber.

Recommendation

Members are asked to note this report.

Main Report

Background

1. The principal legislation governing the management (or 'processing'[1]) of personal information is the Data Protection Act 1998 (DPA). The Act came into effect on 1st March 2000, superseding a previous Act which had only applied to electronic records.

2. The DPA covers all personal information, wherever held in the UK, in whatever medium held. It applies to the whole of the City Corporation, although the following are legally separately responsible for their own compliance with the Act: the City of London Police; the Sir John Cass Foundation Primary School; Members with regard to their Ward work; and the Electoral Registration Officer.

3. The DPA imposes legal obligations on the City Corporation when we hold personal information for our own use; this includes personal information held on our behalf by others ('data processors'). A breach of any of the areas of risk, as defined by the Data Protection (DP) Principles listed in Appendix 2, would be a breach of the Act.

4. In April 2010, the Information Commissioner's powers to fine data controllers (any person or body holding, for their own purposes, other people's personal information) up to £500,000 for breaches of the Act came into force; this was in addition to other enforcement action already available to the Commissioner. Appendix 3 summarises the enforcement powers and action. Fines are issued under formal Monetary Penalty Notices, and cannot be insured against.

5. In the City Corporation, DP compliance is monitored and guided centrally by an Information Officer and Assistant Information Officer, working with an Access to Information Network. This resourcing of DP compliance is shared with the resourcing of compliance with the Freedom of Information Act 2000 (FOIA), which applies to our City Fund functions; and the Environmental Information Regulations 2004 (EIRs), which can apply more widely.

The nature of the risk

6. Given that personal data is continuously processed within the City Corporation in large quantities, in a wide range of ways, and in any medium, a list of particular risks can never be exhaustive.

7. Analysis of the Commissioner's Monetary Penalty Notices shows that the main risks are not sophisticated. They are generally:

   - basic negligence in managing email (and fax) addresses;
   - failing to encrypt;
   - failings in hard copy posting, filing, and disposing of personal information; and

[1] Processing' covers anything which is done with personal information

- allowing theft or loss of personal information outside an authority's premises, in hard copy or on laptops, USB sticks, etc.

8. At the City Corporation, emailing, posting, filing and destruction of personal information are continual processes, and the use of e-devices outside our premises is routine. The risk is increased when the 'processing' is outsourced, as illustrated by the highest fine noted in Appendix 3, which resulted from the activities of a contractor, and was exacerbated by the failure to have a personal data processing agreement in place.

9. Certain service areas are more risk prone than others, due to their need to hold and manage large amounts of personal information. Based on the Commissioner's Monetary Penalty Notices, the highest risk relates to information processed by social services. Other areas at risk include the IS function, which processes vast amounts of personal information electronically; HR; Payroll and Pensions; City schools, and the GSMD.

10. Although the records management and archive repositories probably contain the great majority of the personal information held by the City in hard copy format, these repositories are professionally managed with a high level of security in the storage and movement of records. The risk of a breach in this area, therefore, is low.

11. The key mitigations available are training, awareness raising, monitoring, and IT security measures, including encryption of all e-devices.

12. A related risk to that of a DP breach is to be over-cautious in sharing personal information where release of the information could prove vital to life. Such cases usually become high profile through the media. It is not considered, at this stage, that this would constitute a significant risk for the City Corporation.

13. All breaches, or potential breaches[2], reported to the Information Officer or Assistant Information Officer are logged. Since May 2010, 79 breaches and potential breaches have been logged. Of these, 59 were considered not proven, and of these, 56 related to lost or stolen mobiles and Blackberries (and one iPad). Of the remaining breaches, 18 were cases of proven breach, and 2 of presumed breach.

14. Most of the 18 proven breaches related to accidental disclosure of non-sensitive personal information (within the meaning of the DPA) to unintended recipients. The most common failure (9 cases) was the failure to blind copy ('bcc') the names of third parties in external emails to multiple recipients, e.g. during consultation exercises.

15. The 2 presumed breaches related to unencrypted laptops which were not issued by the City Corporation but, nevertheless, contained City Corporation information, including some personal information.

Mitigating controls: Governance Arrangements

16. Appropriate governance arrangements are the founding mitigating factor in managing this risk. The senior officer responsible for monitoring DP compliance is the Assistant Town Clerk, Peter Nelson, supported, from 2003,

[2] Potential breaches' are where breaches are not proven even though the circumstances may suggest it.

by an Information Officer, who was given responsibility for DP (as Data Protection Officer), FOI compliance, and EIRs compliance.

17. In 2011, because the year-on-year increases in FOI requests were causing concern about the resourcing of DP compliance awareness and monitoring, an Assistant Information Officer post was established. In that year, there was a further 41% increase in FOI requests. While, in 2012, the number of requests remained almost exactly the same, this year, a further increase continues to place pressure on resources.

18. In 2003, the Access to Information Network (AIN) was set up, consisting of around 35 officers from across the organisation. In addition to their day-to-day duties, they work with the corporate officers to ensure DPA, FOIA and EIRs compliance in the areas they represent. The responsibilities of the AIN reps include: training and advising colleagues on compliance under the legislation; assisting in tracking and responding to requests for information; notifying the Information Officer of personal data processing in their areas; and being the first point of contact between the Information Officer and departments.

19. The corporate DP Statement was approved in 2001 and is published on the City's website. It affirms commitment to compliance with the DP Principles, nominated officer responsibility, and staff contractual obligations. Our Legal Notices, also published on the website, include a Privacy and Data Protection Statement.

20. The relevant employee policies are: the DP Policy; the Code of Conduct; and the Communication and Information Systems Use Policy. These include guidance on issues such as the use of mobile devices and the approved City encryption software. A Pupil and Parent Data Protection Policy covers DP compliance at the three City Schools and GSMD, all of which have AIN reps.

21. Contracts with third parties on which the Comptroller and City Solicitor's Department advises have, since 2004, routinely included DP processing clauses. AIN reps are made aware as part of their training that any such contracts set up independently of assistance from Comptroller and City Solicitor's Department should include such clauses.

22. The Information Management Strategy, approved in 2009, covers all information in whatever medium held, and makes reference to the DPA and to information security. It is currently being updated. The Information Officer is a member of the corporate Information Governance Management Board, which aims to ensure that City Corporation information systems, policies and procedures are compliant with ISO 27001 (the international Information Security Management System standard) and information legislation.

23. Within Community and Children's Services there is a nominated 'Caldicott Guardian'. The role involves ensuring adherance to the 'Caldicott Principles', laid down in 1997 by the NHS Executive, and extended to councils with social services responsibilities in 2002. In their effect, they duplicate the requirements of the DP Principles.

Mitigating controls: Training, Awareness and Monitoring - Staff

24. The appointment of the Information Officer was the starting point for the provision of central monitoring and guidance. The following is an outline of the main arrangements for training, promoting awareness, and monitoring.

25. The 'Access to Information' pages on the Intranet are, essentially, a manual on DP (and FOI and the EIRs), providing comprehensive guidance and linking to the Information Commissioner's and Government's published guidance.

26. A rolling programme of DP presentations for all staff identified as working with personal information was initiated in September 2011. Given that it was clear that the greatest risk lay within Community and Children's Services, that Department was the first to receive training. Departments are encouraged to make attendance compulsory for staff with high involvement with personal data. One-to-one training is provided for new AIN reps.

27. Completion of a customised DP e-Learning course is a requirement of the staff Code of Conduct for anyone who processes personal information, which effectively means that most officers are required to complete it as part of their terms and conditions of employment. Completion of the course is also a compulsory part of attendance at DP presentations.

28. The IS Division has set up data security e-learning courses, which include reference to DP and, again, staff are required to complete the courses (in this instance in accordance with specified levels of responsibility).

29. The Monetary Penalty Notices are always circulated to key staff. These highlight the most common causes of breaches (usually very obvious errors), the financial and reputational consequences to authorities, and the additional preventative measures the Commissioner requires to be put in place to prevent further breaches. This has led to changes in practice in the City Corporation, for example: the adoption of a secure email system, and a trial of secure document pouches for use when personal information is to be taken outside the office, both by Community and Children's Services; and the roll out of a secure print, scan and photocopy system across the organisation.

30. AIN reps are reminded annually that any breaches in their areas must be reported to them and the Information Officer immediately. Since 2011, all staff in the City Corporation have been sent an annual one page awareness-raising guide, also warning of the possibility of disciplinary action should breaches occur. The guide is also circulated via eLeader and the Intranet. From now on, both of these reminders will be sent six-monthly.

31. DP compliance is on the Induction Checklist for new joiners, who are provided with the staff DP leaflet which provides basic guidance. However, now that DP breaches have been registered as a strategic risk, the profile of DP in the induction process will be reviewed.

Mitigating controls: Training, Awareness and Monitoring - Members

32. All Members in 2003, and all newly elected Members since,have been sent comprehensive DP compliance guidance drawn up by the Comptroller and City Solicitor, covering both their work for the City Corporation and their Ward work. Members undertaking Ward work are data controllers in their own right and legally responsible for their own DP compliance. They would, therefore,

be personally liable for any fine should they breach the DPA when acting in that capacity.

33. All Members have been offered a one-to-one DP session with the Information Officer or Assistant Information Officer, at the same time as having their Notification (a requirement of the DPA) as data controllers within their Ward work arranged for them. Almost all Members have had a one-to-one DP session and almost all have their Notification arranged for them. Three DP training sessions have been arranged for Members this year.

34. The Members' Website includes a DP (and FOI) briefing page. This links to the 'Access to Information' pages, and the DP compliance document, drawn up by the Comptroller and City Solicitor's Department, and provides the Information Officer's contact details should further guidance be needed.

Mitigating controls: IT security measures

35. Comprehensive procedures exist for the encryption of USB sticks and password protection of mobile devices, such as ipads. If, therefore, devices are lost or stolen, any information should remain inaccessible. In addition, staff and Members are required to report such losses as soon as possible to the IS Division, which in turn immediately reports them to the service provider, who immediately terminates service provision. Should there be any delays in reporting by staff or Members to IS Division of loss or theft, this is looked into by the Information Officer or Assistant Information Officer.

Breach Management at the City Corporation

36. Once a breach, or potential breach, is reported, the Information Officer and Assistant Information Officer assist the Department in managing the breach, or potential breach. With regard to lower level breaches (those not approaching the threshold for reporting to the Information Commissioner), this may include: assisting with formal apologies; contacting unintended recipients of information; reinforcing training requirements, and ensuring that staff understand the procedures to be followed to prevent a recurrence.

37. When a breach is considered significant, a detailed investigation report is completed for the Assistant Town Clerk, with a recommendation as to whether the breach meets the Commissioner's requirements for reporting to his office. The first version of the Commissioner's breach reporting guidance was published in March 2008, and since then, the City Corporation has reported two breaches – one known and one potential.

38. The known breach (December 2008) incurred no formal regulatory action, but the City Corporation was put on notice that "…the matter may be revisited if there is another incident in the future". The breach involved sending a large quantity of personal information in hard copy to a recipient to whom it should not have been disclosed. The information was not sensitive personal information, and was accidentally sent only to one recipient.

39. The potential breach (January 2013) involved sensitive personal information held in hard copy. An investigation concluded that it is unlikely that the information reached the public domain, and the Commissioner accepted this conclusion. However, inadequate security procedures came to light and have been addressed.

40. To date, the City Corporation has not incurred any fines or other enforcement action.

Challenges and further action

41. The main challenge in managing risk SR16 is the scale of the risk. The majority of officers and Members process personal information on a daily basis. It is impossible to monitor comprehensively this scale and detail of processing.

42. The Information Commissioner's enforcement action has, nevertheless, targeted the obvious incompetence and oversights which can occur from time to time with this scale and detail of processing, in spite of training, awareness raising and monitoring. Mitigation is, therefore, a constant challenge.

43. By the end of the year, the aim is to initiate a process whereby AIN reps will carry out regular basic audits, reporting the outcomes to the Information Officer and Assistant Information Officer. The senior AIN rep in Community and Children's Services has already begun this process.

44. The Information Governance Management Board is also looking into instituting a formal Protective Data Marking policy, similar to that used by the City Police, which would be an active system of identifying levels of confidentiality (and, therefore, risk) in relation to classes of information when storing and communicating it.

Strategic Risk Ownership

45. The risk owner for Strategic Risk 16 is the Assistant Town Clerk. However, every Department has a responsibility for the information it holds and a shared responsibility for this risk. In November 2002, a report to the Policy and Resources Committee made this clear: "For effective management … it will be necessary for departments to take responsibility for the co-ordinated implementation and management of the FOIA and DPA".

Conclusion

46. The governance structure and the range of training, awareness-raising and monitoring actions warrant assessing the net risk as Amber. Management and staff are becoming more aware of this risk, especially since the rolling programme of DP presentations was initiated.

47. However, it is unlikely that the net risk could move from Amber to Green, given that personal data processing is such a considerable, widespread and routine activity within most of our functions, and the continuing possibility of human error.

Appendices

- Appendix 1 – Risk Supporting Statement: SR16
- Appendix 2 - DP Principles
- Appendix 3 - Enforcement by the Information Commissioner

Peter Nelson, Assistant Town Clerk
T: 020 7332 1413
E: peter.nelson@cityoflondon.gov.uk

Risk Supporting Statement: SR16

Risk Owner: Assistant Town Clerk

Risk	A breach of the Data Protection Act 1998, by any CoL department due to poor compliance or mishandling of personal information, could result in harm to individuals, a monetary penalty of up to £500,000, compliance enforcement action and significant adverse media coverage. **Links to: All Strategic Aims and Key Policy Priorities.**	**Gross Risk**	**R**
		Likelihood	**Impact**
		5	3

Detail	The Information Commissioner regularly uses his powers to impose considerable fines on public authorities for breaches of the Data Protection Act. There is a need to emphasise the importance of Data Protection and improve awareness, compliance and cooperation amongst Members and staff across the organisation.

Specific Threats/Issues	**Mitigating Actions**
Lack of Member and staff awareness of, and engagement with, the DPA. Office moves/relocations increase the possibility of losing or misplacing personal information. Transferring personal information to third parties, e.g. when contracting out services. Incorrect/accidental disclosure or loss of personal information, e.g. when sending personal information using any medium. Insufficient security in place to protect personal information.	Central monitoring & issuing of guidance exists (since 2003), along with nominated senior officer responsibility. - Access to Information network established, with reps across all departments. - DP awareness written into corporate employee policies as a requirement. - Code of Conduct requirement to complete the corporate DPA e-learning course. - Rolling program of tailored DPA training presentations for all staff and Members. - Record of all presentation attendees and e-learning sign-offs kept for audit purposes. - Awareness emails sent biannually to all staff. - Other awareness raising tools used when highlighting key issues. - Some monitoring of data processor contracts to ensure DPA compliance.

Summary	**Net Risk**	**A**
All Members and officers should be aware of the DPA requirements, and ensure full compliance is maintained at all times. Personal information, in whatever format it is held, should be kept secure at all times. Appropriate polices, procedures and tools should be in place, regarding the management of personal information, including where there is a requirement to share, transfer, disclose, transport and destroy it. To further reduce the risks associated with data protection breaches, compliance audits will have to be undertaken across the organisation. The audits can be undertaken by the Town Clerk's Information Officers in conjunction with each department, looking at what personal information is held, what procedures are in place and what improvements need to be made in the handling of personal information. The e-learning training course should continue to be kept up to date and reviewed at regular intervals.	**Likelihood**	**Impact**
	3	3
	Control Evaluation	
	A	

Appendix 2 – DP Principles

The DPA states:

Principle 1
Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless—
(a) at least one of the conditions in Schedule 2 [of the DPA] is met, and
(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 [of the DPA] is also met.

Principle 2
Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

Principle 3
Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

Principle 4
Personal data shall be accurate and, where necessary, kept up to date.

Principle 5
Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

Principle 6
Personal data shall be processed in accordance with the rights of data subjects under this Act.

Principle 7
Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Principle 8
Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Appendix 3 – Enforcement by the Information Commissioner

1. In April 2010 the Commissioner's powers to fine data controllers up to £500,000 for breaches of the DPA came into force. This was in addition to other enforcement action already available, including imposing Undertakings and, in extreme cases, recourse to the courts. Both civil and criminal offences exist under the DPA, and some of the criminal offences have personal liability.

2. The Commissioner also received powers to summarily audit Government departments for DP compliance. The Commissioner continues to call for the extension of these powers, to cover local authorities a he considers there to be an underlying problem with DP compliance in local government. In March 2013, the House of Commons Justice Select Committee supported this call. In evidence to the Committee, the Commissioner stated that compulsory audits could help stop "really stupid basic errors" in local authorities.

3. At the time of writing 21 local authorities have received fines, ranging from £60,000 to £250,000. These breaches fall into the following categories:

    - emailing to the wrong recipients (5)
    - faxing to the wrong recipients (1)
    - loss or theft of unencrypted laptops (3)
    - posting information to the wrong recipients (5)
    - loss or theft of hard copy information (3)
    - non-confidential disposal of hard copy information and failure to encrypt the digitised information or post it securely (1), which incurred the highest fine (this related to staff pension information)
    - disclosing information via hard copy to the wrong recipients because of incorrect hard copy filing (1)
    - disclosing information via hard copy to the wrong recipients because the information was held on a database which was not 'privacy friendly' in its reports/printouts (1)
    - disclosing information via hard copy to third parties due to lack of understanding of legal restraints on data sharing (1)

    Of the fines, 15 relate to the types of information which would be processed by the Department of Community and Children's Services.

4. There has also been increasing pressure from the Commissioner on data controllers to report any DP breaches, and to not do so is to risk undermining relations with the regulator.

5. Under The Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011, reporting of breaches is already compulsory for public electronic communications service providers. The European Commission is currently looking at this for all sectors.

6. Even where fines are not subsequently imposed, a thorough investigation is still likely, and the data controller is highly likely to be required to sign an Undertaking (a legally binding document) to introduce specified and comprehensive measures required to prevent further breaches.

7. Formal action taken by the Commissioner against a named body in relation to failures in DP compliance is publicised on the Commissioner’s website, including through press releases.

8. Demands have been made by some MPs for the introduction of custodial sentencing for breaches of the DPA.